



# National Critical Information Infrastructure Protection Centre

## Common Vulnerabilities and Exposures(CVE) Report

16 - 29 Feb 2020

Vol. 07 No. 04

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<b>Application</b>					
<b>10web</b>					
<b>photo_gallery</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-02-2020	3.5	Multiple stored XSS vulnerabilities exist in the 10Web Photo Gallery plugin before 1.5.46 WordPress. Successful exploitation of this vulnerability would allow a authenticated admin user to inject arbitrary JavaScript code that is viewed by other users. <b>CVE ID : CVE-2020-9335</b>	N/A	A-10W-PHOT-050320/1
<b>Adobe</b>					
<b>after_effects</b>					
Out-of-bounds Write	20-02-2020	10	Adobe After Effects versions 16.1.2 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. <b>CVE ID : CVE-2020-3765</b>	<a href="https://helpx.adobe.com/security/products/after_effects/apsb20-09.html">https://helpx.adobe.com/security/products/after_effects/apsb20-09.html</a>	A-ADO-AFTE-050320/2
<b>media_encoder</b>					
Out-of-bounds Write	20-02-2020	10	Adobe Media Encoder versions 14.0 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . <b>CVE ID : CVE-2020-3764</b>	<a href="https://helpx.adobe.com/security/products/media-encoder/apsb20-10.html">https://helpx.adobe.com/security/products/media-encoder/apsb20-10.html</a>	A-ADO-MEDI-050320/3
<b>aishu</b>					

CVSS Scoring Scale

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<b>anyshare_cloud</b>					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-02-2020	4	AnyShare Cloud 6.0.9 allows authenticated directory traversal to read files, as demonstrated by the interface/downloadwithpath/downloadfile/?filepath=/etc/passwd URI. <b>CVE ID : CVE-2020-8996</b>	N/A	A-AIS-ANYS-050320/4
<b>Apache</b>					
<b>tomcat</b>					
Improper Input Validation	24-02-2020	7.5	When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that may be surprising. In Apache Tomcat 9.0.0.M1 to 9.0.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99, Tomcat shipped with an AJP Connector enabled by default that listened on all configured IP addresses. It was expected (and recommended in the security guide) that this Connector would be disabled if not required. This vulnerability report identified a mechanism that allowed: - returning arbitrary files from anywhere in the web	<a href="https://security.netapp.com/advisory/ntap-20200226-0002/">https://security.netapp.com/advisory/ntap-20200226-0002/</a>	A-APA-TOMC-050320/5

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>application - processing any file in the web application as a JSP Further, if the web application allowed file upload and stored those files within the web application (or the attacker was able to control the content of the web application by some other means) then this, along with the ability to process a file as a JSP, made remote code execution possible. It is important to note that mitigation is only required if an AJP port is accessible to untrusted users. Users wishing to take a defence-in-depth approach and block the vector that permits returning arbitrary files and execution as JSP may upgrade to Apache Tomcat 9.0.31, 8.5.51 or 7.0.100 or later. A number of changes were made to the default AJP Connector configuration in 9.0.31 to harden the default configuration. It is likely that users upgrading to 9.0.31, 8.5.51 or 7.0.100 or later will need to make small changes to their configurations.</p> <p><b>CVE ID : CVE-2020-1938</b></p>		
<b>kylin</b>					
Improper Neutralization of Special Elements	24-02-2020	4	<p>Kylin has some restful apis which will concatenate SQLs with the user input string, a user is likely to be able to</p>	N/A	A-APA-KYLI-050320/6

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			run malicious database queries. <b>CVE ID : CVE-2020-1937</b>		
<b>Apple</b>					
<b>icloud</b>					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted web content may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3825</b>	N/A	A-APP-ICLO-050320/7
Out-of-bounds Read	27-02-2020	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing a maliciously crafted image may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3826</b>	N/A	A-APP-ICLO-050320/8
XML Injection (aka Blind XPath)	27-02-2020	6.8	A buffer overflow was addressed with improved size validation. This issue is fixed in iOS 13.3.1 and	N/A	A-APP-ICLO-050320/9

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection)			iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted XML may lead to an unexpected application termination or arbitrary code execution. <b>CVE ID : CVE-2020-3846</b>		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	4.3	A denial of service issue was addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. A malicious website may be able to cause a denial of service. <b>CVE ID : CVE-2020-3862</b>	N/A	A-APP-ICLO-050320/10
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted web content may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3865</b>	N/A	A-APP-ICLO-050320/11
Improper Neutralizatio	27-02-2020	4.3	A logic issue was addressed with improved state	N/A	A-APP-ICLO-050320/12

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			management. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted web content may lead to universal cross site scripting. <b>CVE ID : CVE-2020-3867</b>		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted web content may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3868</b>	N/A	A-APP-ICLO-050320/13
<b>itunes</b>					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted web content may lead to arbitrary code execution.	N/A	A-APP-ITUN-050320/14

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-3825</b>		
Out-of-bounds Read	27-02-2020	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing a maliciously crafted image may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3826</b>	N/A	A-APP-ITUN-050320/15
XML Injection (aka Blind XPath Injection)	27-02-2020	6.8	A buffer overflow was addressed with improved size validation. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted XML may lead to an unexpected application termination or arbitrary code execution. <b>CVE ID : CVE-2020-3846</b>	N/A	A-APP-ITUN-050320/16
Missing Authorization	27-02-2020	2.1	The issue was addressed with improved permissions logic. This issue is fixed in iTunes for Windows 12.10.4. A user may gain access to protected parts of the file system. <b>CVE ID : CVE-2020-3861</b>	N/A	A-APP-ITUN-050320/17
Improper	27-02-2020	4.3	A denial of service issue was	N/A	A-APP-ITUN-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. A malicious website may be able to cause a denial of service. <b>CVE ID : CVE-2020-3862</b>		050320/18
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted web content may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3865</b>	N/A	A-APP-ITUN-050320/19
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-02-2020	4.3	A logic issue was addressed with improved state management. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted web content may lead to universal cross site scripting. <b>CVE ID : CVE-2020-3867</b>	N/A	A-APP-ITUN-050320/20
Improper	27-02-2020	9.3	Multiple memory corruption	N/A	A-APP-ITUN-

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			issues were addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted web content may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3868</b>		050320/21
<b>safari</b>					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted web content may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3825</b>	N/A	A-APP-SAFA-050320/22
N/A	27-02-2020	4.3	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in Safari 13.0.5. Visiting a malicious website may lead to address bar spoofing. <b>CVE ID : CVE-2020-3833</b>	N/A	A-APP-SAFA-050320/23
Insufficiently Protected	27-02-2020	4.3	The issue was addressed with improved UI handling.	N/A	A-APP-SAFA-050320/24

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, Safari 13.0.5. A local user may unknowingly send a password unencrypted over the network. <b>CVE ID : CVE-2020-3841</b>		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	4.3	A denial of service issue was addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. A malicious website may be able to cause a denial of service. <b>CVE ID : CVE-2020-3862</b>	N/A	A-APP-SAFA-050320/25
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted web content may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3865</b>	N/A	A-APP-SAFA-050320/26
Improper Neutralization of Input During Web Page Generation	27-02-2020	4.3	A logic issue was addressed with improved state management. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for	N/A	A-APP-SAFA-050320/27

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted web content may lead to universal cross site scripting. <b>CVE ID : CVE-2020-3867</b>		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted web content may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3868</b>	N/A	A-APP-SAFA-050320/28
<b>arvato</b>					
<b>skillpipe</b>					
Improper Input Validation	16-02-2020	4	Arvato Skillpipe 3.0 allows attackers to bypass intended print restrictions by deleting <div id="watermark"> from the HTML source code. <b>CVE ID : CVE-2020-9013</b>	N/A	A-ARV-SKIL-050320/29
<b>auieo</b>					
<b>candidats</b>					
Cross-Site Request Forgery (CSRF)	22-02-2020	6.8	CandidATS 2.1.0 is vulnerable to CSRF that allows for an administrator account to be added via the index.php?m=settings&a=addUser URI.	N/A	A-AUI-CAND-050320/30

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-9341</b>		
<b>Avira</b>					
<b>anti-malware_sdk</b>					
Unrestricted Upload of File with Dangerous Type	20-02-2020	4.3	Avira AV Engine before 8.3.54.138 allows virus-detection bypass via a crafted ISO archive. This affects versions before 8.3.54.138 of Antivirus for Endpoint, Antivirus for Small Business, Exchange Security (Gateway), Internet Security Suite for Windows, Prime, Free Security Suite for Windows, and Cross Platform Anti-malware SDK. <b>CVE ID : CVE-2020-9320</b>	N/A	A-AVI-ANTI-050320/31
<b>antivirus_server</b>					
Unrestricted Upload of File with Dangerous Type	20-02-2020	4.3	Avira AV Engine before 8.3.54.138 allows virus-detection bypass via a crafted ISO archive. This affects versions before 8.3.54.138 of Antivirus for Endpoint, Antivirus for Small Business, Exchange Security (Gateway), Internet Security Suite for Windows, Prime, Free Security Suite for Windows, and Cross Platform Anti-malware SDK. <b>CVE ID : CVE-2020-9320</b>	N/A	A-AVI-ANTI-050320/32
<b>avira_antivirus_for_endpoint</b>					
Unrestricted Upload of File with Dangerous Type	20-02-2020	4.3	Avira AV Engine before 8.3.54.138 allows virus-detection bypass via a crafted ISO archive. This affects versions before	N/A	A-AVI-AVIR-050320/33

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			8.3.54.138 of Antivirus for Endpoint, Antivirus for Small Business, Exchange Security (Gateway), Internet Security Suite for Windows, Prime, Free Security Suite for Windows, and Cross Platform Anti-malware SDK. <b>CVE ID : CVE-2020-9320</b>		
<b>avira_antivirus_for_small_business</b>					
Unrestricted Upload of File with Dangerous Type	20-02-2020	4.3	Avira AV Engine before 8.3.54.138 allows virus-detection bypass via a crafted ISO archive. This affects versions before 8.3.54.138 of Antivirus for Endpoint, Antivirus for Small Business, Exchange Security (Gateway), Internet Security Suite for Windows, Prime, Free Security Suite for Windows, and Cross Platform Anti-malware SDK. <b>CVE ID : CVE-2020-9320</b>	N/A	A-AVI-AVIR-050320/34
<b>avira_exchange_security</b>					
Unrestricted Upload of File with Dangerous Type	20-02-2020	4.3	Avira AV Engine before 8.3.54.138 allows virus-detection bypass via a crafted ISO archive. This affects versions before 8.3.54.138 of Antivirus for Endpoint, Antivirus for Small Business, Exchange Security (Gateway), Internet Security Suite for Windows, Prime, Free Security Suite for Windows, and Cross Platform Anti-malware SDK. <b>CVE ID : CVE-2020-9320</b>	N/A	A-AVI-AVIR-050320/35

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<b>avira_free_security_suite</b>					
Unrestricted Upload of File with Dangerous Type	20-02-2020	4.3	Avira AV Engine before 8.3.54.138 allows virus-detection bypass via a crafted ISO archive. This affects versions before 8.3.54.138 of Antivirus for Endpoint, Antivirus for Small Business, Exchange Security (Gateway), Internet Security Suite for Windows, Prime, Free Security Suite for Windows, and Cross Platform Anti-malware SDK. <b>CVE ID : CVE-2020-9320</b>	N/A	A-AVI-AVIR-050320/36
<b>avira_internet_security_suite</b>					
Unrestricted Upload of File with Dangerous Type	20-02-2020	4.3	Avira AV Engine before 8.3.54.138 allows virus-detection bypass via a crafted ISO archive. This affects versions before 8.3.54.138 of Antivirus for Endpoint, Antivirus for Small Business, Exchange Security (Gateway), Internet Security Suite for Windows, Prime, Free Security Suite for Windows, and Cross Platform Anti-malware SDK. <b>CVE ID : CVE-2020-9320</b>	N/A	A-AVI-AVIR-050320/37
<b>avira_prime</b>					
Unrestricted Upload of File with Dangerous Type	20-02-2020	4.3	Avira AV Engine before 8.3.54.138 allows virus-detection bypass via a crafted ISO archive. This affects versions before 8.3.54.138 of Antivirus for Endpoint, Antivirus for Small Business, Exchange Security	N/A	A-AVI-AVIR-050320/38

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(Gateway), Internet Security Suite for Windows, Prime, Free Security Suite for Windows, and Cross Platform Anti-malware SDK. <b>CVE ID : CVE-2020-9320</b>		
<b>Blackboard</b>					
<b>blackboard_learn</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-02-2020	3.5	Stored Cross-site scripting (XSS) vulnerability in Blackboard Learn/PeopleTool v9.1 allows users to inject arbitrary web script via the Tile widget in the People Tool profile editor. <b>CVE ID : CVE-2020-9008</b>	N/A	A-BLA-BLAC-050320/39
<b>Broadcom</b>					
<b>unified_infrastructure_management</b>					
Improper Input Validation	18-02-2020	10	CA Unified Infrastructure Management (Nimsoft/UIM) 9.20 and below contains an improper ACL handling vulnerability in the robot (controller) component. A remote attacker can execute commands, read from, or write to the target system. <b>CVE ID : CVE-2020-8010</b>	<a href="https://techdocs.broadcom.com/content/status/announcement-documents/2019/ca20200205-01-security-notice-for-ca-unified-infrastructure-management.html">https://techdocs.broadcom.com/content/status/announcement-documents/2019/ca20200205-01-security-notice-for-ca-unified-infrastructure-management.html</a>	A-BRO-UNIF-050320/40
NULL Pointer	18-02-2020	5	CA Unified Infrastructure Management (Nimsoft/UIM)	<a href="https://techdocs.broadcom.com/content/status/announcement-documents/2019/ca20200205-01-security-notice-for-ca-unified-infrastructure-management.html">https://techdocs.broadcom.com/content/status/announcement-documents/2019/ca20200205-01-security-notice-for-ca-unified-infrastructure-management.html</a>	A-BRO-UNIF-050320/41

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			9.20 and below contains a null pointer dereference vulnerability in the robot (controller) component. A remote attacker can crash the Controller service. <b>CVE ID : CVE-2020-8011</b>	com.com/us/product-content/status/announcement-documents/2019/ca20200205-01-security-notice-for-ca-unified-infrastructure-management.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-02-2020	7.5	CA Unified Infrastructure Management (Nimsoft/UIM) 9.20 and below contains a buffer overflow vulnerability in the robot (controller) component. A remote attacker can execute arbitrary code. <b>CVE ID : CVE-2020-8012</b>	https://techdocs.broadcom.com/us/product-content/status/announcement-documents/2019/ca20200205-01-security-notice-for-ca-unified-infrastructure-management.html	A-BRO-UNIF-050320/42
<b>Buddypress</b>					
<b>buddypress</b>					
Information Exposure	24-02-2020	5	In BuddyPress before 5.1.2, requests to a certain REST API endpoint can result in private user data getting exposed. Authentication is not needed. This has been	https://github.com/buddypress/Buddypress/security/advisories/GHS	A-BUD-BUDD-050320/43

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			patched in version 5.1.2. <b>CVE ID : CVE-2020-5244</b>	A-3j78-7m59-r7gv	
<b>Cacti</b>					
<b>cacti</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-02-2020	9.3	graph_realtime.php in Cacti 1.2.8 allows remote attackers to execute arbitrary OS commands via shell metacharacters in a cookie, if a guest user has the graph real-time privilege. <b>CVE ID : CVE-2020-8813</b>	<a href="https://github.com/Cacti/cacti/issues/3285">https://github.com/Cacti/cacti/issues/3285</a>	A-CAC-CACT-050320/44
<b>Centreon</b>					
<b>centreon</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-02-2020	9	Centreon 19.10 allows remote authenticated users to execute arbitrary OS commands via shell metacharacters in the server_ip field in JSON data in an api/internal.php?object=centreon_configuration_remote request. <b>CVE ID : CVE-2020-9463</b>	N/A	A-CEN-CENT-050320/45
<b>ciprianmp</b>					
<b>phpmychat-plus</b>					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-02-2020	6.4	phpMyChat-Plus 1.98 is vulnerable to multiple SQL injections against the deluser.php Delete User functionality, as demonstrated by pmc_username. <b>CVE ID : CVE-2020-9265</b>	N/A	A-CIP-PHPM-050320/46

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<b>Cisco</b>					
<b>enterprise_network_function_virtualization_infrastructure</b>					
Improper Verification of Cryptographic Signature	19-02-2020	7.2	<p>A vulnerability in the upgrade component of Cisco Enterprise NFW Infrastructure Software (NFWIS) could allow an authenticated, local attacker to install a malicious file when upgrading. The vulnerability is due to insufficient signature validation. An attacker could exploit this vulnerability by providing a crafted upgrade file. A successful exploit could allow the attacker to upload crafted code to the affected device.</p> <p><b>CVE ID : CVE-2020-3138</b></p>	N/A	A-CIS-ENTE-050320/47
<b>finesse</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-02-2020	4.3	<p>A vulnerability in the web-based management interface of Cisco Finesse could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of the affected software. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a malicious link. A successful exploit could allow the</p>	N/A	A-CIS-FINE-050320/48

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. <b>CVE ID : CVE-2020-3159</b>		
<b>anyconnect_secure_mobility_client</b>					
Uncontrolled Search Path Element	19-02-2020	4.9	A vulnerability in the installer component of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated local attacker to copy user-supplied files to system level directories with system level privileges. The vulnerability is due to the incorrect handling of directory paths. An attacker could exploit this vulnerability by creating a malicious file and copying the file to a system directory. An exploit could allow the attacker to copy malicious files to arbitrary locations with system level privileges. This could include DLL pre-loading, DLL hijacking, and other related attacks. To exploit this vulnerability, the attacker needs valid credentials on the Windows system. <b>CVE ID : CVE-2020-3153</b>	N/A	A-CIS-ANYC-050320/49
<b>adaptive_security_appliance_software</b>					
Improper Neutralization of Special Elements	26-02-2020	7.2	A vulnerability in the CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an	N/A	A-CIS-ADAP-050320/50

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			<p>authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS). The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges.</p> <p><b>CVE ID : CVE-2020-3167</b></p>		
<b>data_center_network_manager</b>					
Improper Privilege Management	19-02-2020	6.5	<p>A vulnerability in the REST API endpoint of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker to elevate privileges on the application. The vulnerability is due to insufficient access control validation. An attacker could exploit this vulnerability by authenticating with a low-privilege account and sending a crafted request to the API. A successful exploit</p>	N/A	A-CIS-DATA-050320/51

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to interact with the API with administrative privileges. <b>CVE ID : CVE-2020-3112</b>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-02-2020	3.5	A vulnerability in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information. <b>CVE ID : CVE-2020-3113</b>	N/A	A-CIS-DATA-050320/52
Cross-Site Request Forgery (CSRF)	19-02-2020	6.8	A vulnerability in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. The vulnerability is due to	N/A	A-CIS-DATA-050320/53

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>insufficient CSRF protections for the web-based management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link while having an active session on an affected device. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user.</p> <p><b>CVE ID : CVE-2020-3114</b></p>		
<b>email_security_appliance</b>					
Uncontrolled Resource Consumption	19-02-2020	7.1	<p>A vulnerability in the email message scanning feature of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to cause a temporary denial of service (DoS) condition on an affected device. The vulnerability is due to inadequate parsing mechanisms for specific email body components. An attacker could exploit this vulnerability by sending a malicious email containing a high number of shortened URLs through an affected device. A successful exploit could allow the attacker to consume processing resources, causing a DoS</p>	N/A	A-CIS-EMAI-050320/54

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			condition on an affected device. To successfully exploit this vulnerability, certain conditions beyond the control of the attacker must occur. <b>CVE ID : CVE-2020-3132</b>		
<b>firepower_threat_defense</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	A vulnerability in the CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS). The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges. <b>CVE ID : CVE-2020-3167</b>	N/A	A-CIS-FIRE-050320/55
<b>identity_services_engine</b>					
Improper Neutralization	19-02-2020	4.3	A vulnerability in the logging component of Cisco Identity	N/A	A-CIS-IDEN-050320/56

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			<p>Services Engine could allow an unauthenticated remote attacker to conduct cross-site scripting attacks. The vulnerability is due to the improper validation of endpoint data stored in logs used by the web-based interface. An attacker could exploit this vulnerability by sending malicious endpoint data to the targeted system. An exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or to access sensitive, browser-based information.</p> <p><b>CVE ID : CVE-2020-3156</b></p>		
<b>meeting_server</b>					
Improper Input Validation	19-02-2020	4.3	<p>A vulnerability in the Extensible Messaging and Presence Protocol (XMPP) feature of Cisco Meeting Server software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition for users of XMPP conferencing applications. Other applications and processes are unaffected. The vulnerability is due to improper input validation of XMPP packets. An attacker could exploit this vulnerability by sending crafted XMPP packets to an affected device. An exploit could allow the attacker to</p>	N/A	A-CIS-MEET-050320/57

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cause process crashes and a DoS condition for XMPP conferencing applications. <b>CVE ID : CVE-2020-3160</b>		
<b>cloud_email_security</b>					
Uncontrolled Resource Consumption	19-02-2020	7.1	A vulnerability in the email message scanning feature of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to cause a temporary denial of service (DoS) condition on an affected device. The vulnerability is due to inadequate parsing mechanisms for specific email body components. An attacker could exploit this vulnerability by sending a malicious email containing a high number of shortened URLs through an affected device. A successful exploit could allow the attacker to consume processing resources, causing a DoS condition on an affected device. To successfully exploit this vulnerability, certain conditions beyond the control of the attacker must occur. <b>CVE ID : CVE-2020-3132</b>	N/A	A-CIS-CLOU-050320/58
<b>cloud_web_security</b>					
Improper Neutralization of Special	19-02-2020	4	A vulnerability in the web UI of Cisco Cloud Web Security (CWS) could allow an	N/A	A-CIS-CLOU-050320/59

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			authenticated, remote attacker to execute arbitrary SQL queries. The vulnerability exists because the web-based management interface improperly validates SQL values. An authenticated attacker could exploit this vulnerability sending malicious requests to the affected device. An exploit could allow the attacker to modify values on or return values from the underlying database. <b>CVE ID : CVE-2020-3154</b>		
<b>smart_software_manager_on-prem</b>					
Use of Hard-coded Credentials	19-02-2020	8.8	A vulnerability in the High Availability (HA) service of Cisco Smart Software Manager On-Prem could allow an unauthenticated, remote attacker to access a sensitive part of the system with a high-privileged account. The vulnerability is due to a system account that has a default and static password and is not under the control of the system administrator. An attacker could exploit this vulnerability by using this default account to connect to the affected system. A successful exploit could allow the attacker to obtain read and write access to system data, including the configuration of an affected	N/A	A-CIS-SMAR-050320/60

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. The attacker would gain access to a sensitive portion of the system, but the attacker would not have full administrative rights to control the device. <b>CVE ID : CVE-2020-3158</b>		
<b>unified_contact_center_enterprise</b>					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	19-02-2020	7.1	A vulnerability in the Live Data server of Cisco Unified Contact Center Enterprise could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability exists because the affected software improperly manages resources when processing inbound Live Data traffic. An attacker could exploit this vulnerability by sending multiple crafted Live Data packets to an affected device. A successful exploit could cause the affected device to run out of buffer resources, which could result in a stack overflow and cause the affected device to reload, resulting in a DoS condition. Note: The Live Data port in Cisco Unified Contact Center Enterprise devices allows only a single TCP connection. To exploit this vulnerability, an attacker would have to send crafted packets to an affected device before a	N/A	A-CIS-UNIF-050320/61

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			legitimate Live Data client establishes a connection. <b>CVE ID : CVE-2020-3163</b>		
<b>ucs_manager</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	A vulnerability in the CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS). The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges. <b>CVE ID : CVE-2020-3167</b>	N/A	A-CIS-UCS_-050320/62
Improper Neutralization of Special Elements used in an OS Command ('OS Command	26-02-2020	7.2	A vulnerability in the local management (local-mgmt) CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the	N/A	A-CIS-UCS_-050320/63

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			<p>underlying operating system (OS) of an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges.</p> <p><b>CVE ID : CVE-2020-3171</b></p>		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	<p>A vulnerability in the local management (local-mgmt) CLI of Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) on an affected device. The vulnerability is due to insufficient input validation of command arguments. An attacker could exploit this vulnerability by including crafted arguments to specific commands on the local management CLI. A successful exploit could allow the attacker to execute</p>	N/A	A-CIS-UCS_-050320/64

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges. <b>CVE ID : CVE-2020-3173</b>		
<b>cloudfoundry</b>					
<b>routing_release</b>					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	27-02-2020	5	Cloud Foundry Routing Release, versions prior to 0.197.0, contains GoRouter, which allows malicious clients to send invalid headers, causing caching layers to reject subsequent legitimate clients trying to access the app. <b>CVE ID : CVE-2020-5401</b>	<a href="https://www.cloudfoundry.org/blog/cve-2020-5401">https://www.cloudfoundry.org/blog/cve-2020-5401</a>	A-CLO-ROUT-050320/65
<b>cf-deployment</b>					
Information Exposure Through Log Files	27-02-2020	4	Cloud Foundry Cloud Controller (CAPI), versions prior to 1.91.0, logs properties of background jobs when they are run, which may include sensitive information such as credentials if provided to the job. A malicious user with access to those logs may gain unauthorized access to resources protected by such credentials.	<a href="https://www.cloudfoundry.org/blog/cve-2020-5400">https://www.cloudfoundry.org/blog/cve-2020-5400</a>	A-CLO-CF-D-050320/66

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-5400</b>		
Cross-Site Request Forgery (CSRF)	27-02-2020	6.8	In Cloud Foundry UAA, versions prior to 74.14.0, a CSRF vulnerability exists due to the OAuth2 state parameter not being checked in the callback function when authenticating with external identity providers. <b>CVE ID : CVE-2020-5402</b>	<a href="https://www.cloudfoundry.org/blog/cve-2020-5402">https://www.cloudfoundry.org/blog/cve-2020-5402</a>	A-CLO-CF-D-050320/67
<b>cloud_controller</b>					
Information Exposure Through Log Files	27-02-2020	4	Cloud Foundry Cloud Controller (CAPI), versions prior to 1.91.0, logs properties of background jobs when they are run, which may include sensitive information such as credentials if provided to the job. A malicious user with access to those logs may gain unauthorized access to resources protected by such credentials. <b>CVE ID : CVE-2020-5400</b>	<a href="https://www.cloudfoundry.org/blog/cve-2020-5400">https://www.cloudfoundry.org/blog/cve-2020-5400</a>	A-CLO-CLOU-050320/68
<b>user_account_and_authentication</b>					
Cross-Site Request Forgery (CSRF)	27-02-2020	6.8	In Cloud Foundry UAA, versions prior to 74.14.0, a CSRF vulnerability exists due to the OAuth2 state parameter not being checked in the callback function when authenticating with external identity providers. <b>CVE ID : CVE-2020-5402</b>	<a href="https://www.cloudfoundry.org/blog/cve-2020-5402">https://www.cloudfoundry.org/blog/cve-2020-5402</a>	A-CLO-USER-050320/69
<b>codecov</b>					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<b>codecov</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-02-2020	6.5	codecov-node npm module before 3.6.5 allows remote attackers to execute arbitrary commands. The value provided as part of the gcov-root argument is executed by the exec function within lib/codecov.js. This vulnerability exists due to an incomplete fix of CVE-2020-7596. <b>CVE ID : CVE-2020-7597</b>	N/A	A-COD-CODE-050320/70
<b>Codologic</b>					
<b>codoforum</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-02-2020	3.5	Codoforum 4.8.8 allows self-XSS via the title of a new topic. <b>CVE ID : CVE-2020-9007</b>	N/A	A-COD-CODO-050320/71
<b>coturn_project</b>					
<b>coturn</b>					
Out-of-bounds Write	19-02-2020	7.5	An exploitable heap overflow vulnerability exists in the way CoTURN 4.5.1.1 web server parses POST requests. A specially crafted HTTP POST request can lead to information leaks and other misbehavior. An attacker needs to send an HTTPS request to trigger this vulnerability. <b>CVE ID : CVE-2020-6061</b>	N/A	A-COT-COTU-050320/72

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	19-02-2020	5	An exploitable denial-of-service vulnerability exists in the way CoTURN 4.5.1.1 web server parses POST requests. A specially crafted HTTP POST request can lead to server crash and denial of service. An attacker needs to send an HTTP request to trigger this vulnerability. <b>CVE ID : CVE-2020-6062</b>	N/A	A-COT-COTU-050320/73
<b>couchbase</b>					
<b>couchbase_server</b>					
Incorrect Default Permissions	22-02-2020	7.5	Couchbase Server 4.x and 5.x before 6.0.0 has Insecure Permissions for the projector and indexer REST endpoints (they allow unauthenticated access). <b>CVE ID : CVE-2020-9039</b>	<a href="https://www.couchbase.com/resources/security#SecurityAlerts">https://www.couchbase.com/resources/security#SecurityAlerts</a>	A-COU-COUC-050320/74
<b>dnnsoftware</b>					
<b>dotnetnuke</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-02-2020	3.5	DNN (formerly DotNetNuke) through 9.4.4 allows XSS (issue 1 of 2). <b>CVE ID : CVE-2020-5186</b>	N/A	A-DNN-DOTN-050320/75
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-02-2020	6.5	DNN (formerly DotNetNuke) through 9.4.4 allows Path Traversal (issue 2 of 2). <b>CVE ID : CVE-2020-5187</b>	N/A	A-DNN-DOTN-050320/76

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	24-02-2020	4	DNN (formerly DotNetNuke) through 9.4.4 has Insecure Permissions. <b>CVE ID : CVE-2020-5188</b>	N/A	A-DNN-DOTN-050320/77
<b>Dolibarr</b>					
<b>dolibarr</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-02-2020	3.5	Dolibarr 11.0 allows XSS via the joinfiles, topic, or code parameter, or the HTTP Referer header. <b>CVE ID : CVE-2020-9016</b>	N/A	A-DOL-DOLI-050320/78
<b>Emerson</b>					
<b>openenterprise_scada_server</b>					
Out-of-bounds Write	19-02-2020	7.5	A Heap-based Buffer Overflow was found in Emerson OpenEnterprise SCADA Server 2.83 (if Modbus or ROC Interfaces have been installed and are in use) and all versions of OpenEnterprise 3.1 through 3.3.3, where a specially crafted script could execute code on the OpenEnterprise Server. <b>CVE ID : CVE-2020-6970</b>	N/A	A-EME-OPEN-050320/79
<b>enviragallery</b>					
<b>photo_gallery</b>					
Improper Neutralization of Input During Web Page Generation	25-02-2020	3.5	A stored XSS vulnerability exists in the Envira Photo Gallery plugin through 1.7.6 for WordPress. Successful exploitation of this vulnerability would allow a	N/A	A-ENV-PHOT-050320/80

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			authenticated low-privileged user to inject arbitrary JavaScript code that is viewed by other users. <b>CVE ID : CVE-2020-9334</b>		
<b>Eset</b>					
<b>cyber_security</b>					
Improper Input Validation	18-02-2020	4.3	ESET Archive Support Module before 1296 allows virus-detection bypass via a crafted Compression Information Field in a ZIP archive. This affects versions before 1294 of Smart Security Premium, Internet Security, NOD32 Antivirus, Cyber Security Pro (macOS), Cyber Security (macOS), Mobile Security for Android, Smart TV Security, and NOD32 Antivirus 4 for Linux Desktop. <b>CVE ID : CVE-2020-9264</b>	N/A	A-ESE-CYBE-050320/81
<b>internet_security</b>					
Improper Input Validation	18-02-2020	4.3	ESET Archive Support Module before 1296 allows virus-detection bypass via a crafted Compression Information Field in a ZIP archive. This affects versions before 1294 of Smart Security Premium, Internet Security, NOD32 Antivirus, Cyber Security Pro (macOS), Cyber Security (macOS), Mobile Security for Android, Smart TV Security, and NOD32 Antivirus 4 for Linux Desktop.	N/A	A-ESE-INTE-050320/82

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-9264</b>		
<b>mobile_security</b>					
Improper Input Validation	18-02-2020	4.3	ESET Archive Support Module before 1296 allows virus-detection bypass via a crafted Compression Information Field in a ZIP archive. This affects versions before 1294 of Smart Security Premium, Internet Security, NOD32 Antivirus, Cyber Security Pro (macOS), Cyber Security (macOS), Mobile Security for Android, Smart TV Security, and NOD32 Antivirus 4 for Linux Desktop. <b>CVE ID : CVE-2020-9264</b>	N/A	A-ESE-MOBI-050320/83
<b>nod32_antivirus</b>					
Improper Input Validation	18-02-2020	4.3	ESET Archive Support Module before 1296 allows virus-detection bypass via a crafted Compression Information Field in a ZIP archive. This affects versions before 1294 of Smart Security Premium, Internet Security, NOD32 Antivirus, Cyber Security Pro (macOS), Cyber Security (macOS), Mobile Security for Android, Smart TV Security, and NOD32 Antivirus 4 for Linux Desktop. <b>CVE ID : CVE-2020-9264</b>	N/A	A-ESE-NOD3-050320/84
<b>smart_security</b>					
Improper Input	18-02-2020	4.3	ESET Archive Support Module before 1296 allows virus-detection bypass via a	N/A	A-ESE-SMAR-050320/85

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			crafted Compression Information Field in a ZIP archive. This affects versions before 1294 of Smart Security Premium, Internet Security, NOD32 Antivirus, Cyber Security Pro (macOS), Cyber Security (macOS), Mobile Security for Android, Smart TV Security, and NOD32 Antivirus 4 for Linux Desktop. <b>CVE ID : CVE-2020-9264</b>		
<b>smart_tv_security</b>					
Improper Input Validation	18-02-2020	4.3	ESET Archive Support Module before 1296 allows virus-detection bypass via a crafted Compression Information Field in a ZIP archive. This affects versions before 1294 of Smart Security Premium, Internet Security, NOD32 Antivirus, Cyber Security Pro (macOS), Cyber Security (macOS), Mobile Security for Android, Smart TV Security, and NOD32 Antivirus 4 for Linux Desktop. <b>CVE ID : CVE-2020-9264</b>	N/A	A-ESE-SMAR-050320/86
<b>export_users_to_csv_project</b>					
<b>export_users_to_csv</b>					
Improper Neutralization of Special Elements in Output Used by a Downstream	28-02-2020	5.8	The Export Users to CSV plugin through 1.4.2 for WordPress allows CSV Injection. <b>CVE ID : CVE-2020-9466</b>	N/A	A-EXP-EXPO-050320/87

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Component ('Injection')					
<b>fauzantrif_election_project</b>					
<b>fauzantrif_election</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-02-2020	3.5	fauzantrif eLecture 2.0 has XSS via the Admin Dashboard -> Settings -> Election -> "message if election is closed" field. <b>CVE ID : CVE-2020-9336</b>	N/A	A-FAU-FAUZ-050320/88
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-02-2020	6.5	fauzantrif eLecture 2.0 has SQL Injection via the admin/ajax/op_kandidat.php id parameter. <b>CVE ID : CVE-2020-9340</b>	N/A	A-FAU-FAUZ-050320/89
<b>fiserv</b>					
<b>accurate_reconciliation</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-02-2020	3.5	Fiserv Accurate Reconciliation 2.19.0 allows XSS via the Source or Destination field of the Configuration Manager (Configuration Parameter Translation) page. <b>CVE ID : CVE-2020-8951</b>	N/A	A-FIS-ACCU-050320/90
Improper Neutralization of Input During Web Page Generation ('Cross-site	26-02-2020	4.3	Fiserv Accurate Reconciliation 2.19.0 allows XSS via the logout.jsp timeOut parameter. <b>CVE ID : CVE-2020-8952</b>	N/A	A-FIS-ACCU-050320/91

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')					
<b>Gitlab</b>					
<b>gitlab</b>					
Missing Authorization	17-02-2020	5	In GitLab Enterprise Edition (EE) 12.5.0 through 12.7.5, sharing a group with a group could grant project access to unauthorized users. <b>CVE ID : CVE-2020-8795</b>	<a href="https://about.gitlab.com/releases/2020/02/13/critical-security-release-gitlab-12-dot-7-dot-6-released/">https://about.gitlab.com/releases/2020/02/13/critical-security-release-gitlab-12-dot-7-dot-6-released/</a>	A-GIT-GITL-050320/92
<b>gluu</b>					
<b>gluu_server</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-02-2020	4.3	A cross-site scripting (XSS) vulnerability in the Import People functionality in Gluu Identity Configuration 4.0 allows remote attackers to inject arbitrary web script or HTML via the filename parameter. <b>CVE ID : CVE-2020-9012</b>	N/A	A-GLU-GLUU-050320/93
<b>GNU</b>					
<b>screen</b>					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-02-2020	7.5	A buffer overflow was found in the way GNU Screen before 4.8.0 treated the special escape OSC 49. Specially crafted output, or a special program, could corrupt memory and crash Screen or possibly have unspecified other impact. <b>CVE ID : CVE-2020-9366</b>	N/A	A-GNU-SCRE-050320/94
<b>gogs</b>					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<b>gogs</b>					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	21-02-2020	4.3	Gogs through 0.11.91 allows attackers to violate the admin-specified repo-creation policy due to an internal/db/repo.go race condition. <b>CVE ID : CVE-2020-9329</b>	N/A	A-GOG-GOGS-050320/95
<b>golfbuddyglobal</b>					
<b>course_manager</b>					
Insufficiently Protected Credentials	26-02-2020	4	In GolfBuddy Course Manager 1.1, passwords are sent (with base64 encoding) via a GET request. <b>CVE ID : CVE-2020-9337</b>	N/A	A-GOL-COUR-050320/96
<b>Google</b>					
<b>chrome</b>					
Access of Resource Using Incompatible Type ('Type Confusion')	27-02-2020	6.8	Type confusion in V8 in Google Chrome prior to 80.0.3987.116 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. <b>CVE ID : CVE-2020-6383</b>	N/A	A-GOO-CHRO-050320/97
Use After Free	27-02-2020	6.8	Use after free in WebAudio in Google Chrome prior to 80.0.3987.116 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. <b>CVE ID : CVE-2020-6384</b>	N/A	A-GOO-CHRO-050320/98
Use After Free	27-02-2020	6.8	Use after free in speech in Google Chrome prior to	N/A	A-GOO-CHRO-050320/99

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			80.0.3987.116 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. <b>CVE ID : CVE-2020-6386</b>		
Out-of-bounds Write	27-02-2020	6.8	Out of bounds memory access in streams in Google Chrome prior to 80.0.3987.122 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. <b>CVE ID : CVE-2020-6407</b>	N/A	A-GOO-CHRO-050320/100
Access of Resource Using Incompatible Type ('Type Confusion')	27-02-2020	4.3	Type confusion in V8 in Google Chrome prior to 80.0.3987.122 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. <b>CVE ID : CVE-2020-6418</b>	N/A	A-GOO-CHRO-050320/101
<b>gurux</b>					
<b>device_language_message_specification_director</b>					
Download of Code Without Integrity Check	25-02-2020	6.8	Gurux GXDLMS Director prior to 8.5.1905.1301 downloads updates to add-ins and OBIS code over an unencrypted HTTP connection. A man-in-the-middle attacker can prompt the user to download updates by modifying the contents of gurux.fi/obis/files.xml and gurux.fi/updates/updates.xml. Then, the attacker can modify the contents of	N/A	A-GUR-DEVI-050320/102

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			downloaded files. In the case of add-ins (if the user is using those), this will lead to code execution. In case of OBIS codes (which the user is always using as they are needed to communicate with the energy meters), this can lead to code execution when combined with CVE-2020-8810. <b>CVE ID : CVE-2020-8809</b>		
<b>gwtupload_project</b>					
<b>gwtupload</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-02-2020	4.3	The file-upload feature in GwtUpload 1.0.3 allows XSS via a crafted filename. <b>CVE ID : CVE-2020-9447</b>	N/A	A-GWT-GWTU-050320/103
<b>Horde</b>					
<b>groupware</b>					
Improper Control of Generation of Code ('Code Injection')	17-02-2020	7.5	Horde Groupware Webmail Edition 5.2.22 allows injection of arbitrary PHP code via CSV data, leading to remote code execution. <b>CVE ID : CVE-2020-8518</b>	<a href="https://lists.horde.org/archives/announce/2020/001285.html">https://lists.horde.org/archives/announce/2020/001285.html</a>	A-HOR-GROU-050320/104
<b>Huawei</b>					
<b>pcmanager</b>					
Improper Privilege Management	28-02-2020	4.6	PCManager with versions earlier than 10.0.5.51 have a privilege escalation vulnerability in Huawei PCManager products. An authenticated, local attacker	N/A	A-HUA-PCMA-050320/105

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can perform specific operation to exploit this vulnerability. Successful exploitation may cause the attacker to obtain a higher privilege. <b>CVE ID : CVE-2020-1844</b>		
<b>gaussdb_200</b>					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-02-2020	6.5	GaussDB 200 with version of 6.5.1 have a command injection vulnerability. The software constructs part of a command using external input from users, but the software does not sufficiently validate the user input. Successful exploit could allow the attacker to inject certain commands. <b>CVE ID : CVE-2020-1790</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-gauss-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-gauss-en</a>	A-HUA-GAUS-050320/106
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-02-2020	6.5	GaussDB 200 with version of 6.5.1 have a command injection vulnerability. Due to insufficient input validation, remote attackers with low permissions could exploit this vulnerability by sending crafted commands to the affected device. Successful exploit could allow an attacker to execute commands. <b>CVE ID : CVE-2020-1811</b>	<a href="https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200120-01-gaussdb200-en">https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200120-01-gaussdb200-en</a>	A-HUA-GAUS-050320/107
Improper Limitation of a Pathname to a Restricted Directory	17-02-2020	4	GaussDB 200 with version of 6.5.1 have a path traversal vulnerability. Due to insufficient input path validation, an authenticated attacker can traverse	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-</a>	A-HUA-GAUS-050320/108

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			directories and download files to a specific directory. Successful exploit may cause information leakage. <b>CVE ID : CVE-2020-1853</b>	20200120-01-path-en	
<b>iblssoft</b>					
<b>online_weather</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-02-2020	4.3	IBL Online Weather before 4.3.5a allows unauthenticated reflected XSS via the redirect page. <b>CVE ID : CVE-2020-9405</b>	N/A	A-IBL-ONLI-050320/109
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	26-02-2020	7.5	IBL Online Weather before 4.3.5a allows unauthenticated eval injection via the queryBCP method of the Auxiliary Service. <b>CVE ID : CVE-2020-9406</b>	N/A	A-IBL-ONLI-050320/110
Information Exposure	26-02-2020	5	IBL Online Weather before 4.3.5a allows attackers to obtain sensitive information by reading the IWEBSERVICE_JSONRPC_COOKIE cookie. <b>CVE ID : CVE-2020-9407</b>	N/A	A-IBL-ONLI-050320/111
<b>IBM</b>					
<b>db2</b>					
Uncontrolled Resource Consumption	19-02-2020	5	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow an unauthenticated	<a href="https://www.ibm.com/support/pages/node/2876307">https://www.ibm.com/support/pages/node/2876307</a>	A-IBM-DB2-050320/112

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user to send specially crafted packets to cause a denial of service from excessive memory usage. <b>CVE ID : CVE-2020-4135</b>		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-02-2020	4	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.5 could allow an authenticated attacker to cause a denial of service due to incorrect handling of certain commands. IBM X-Force ID: 174341. <b>CVE ID : CVE-2020-4161</b>	<a href="https://www.ibm.com/support/pages/node/2874621">https://www.ibm.com/support/pages/node/2874621</a>	A-IBM-DB2-050320/113
N/A	19-02-2020	4	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 10.5, 11.1, and 11.5 could allow an authenticated attacker to send specially crafted commands to cause a denial of service. IBM X-Force ID: 174914. <b>CVE ID : CVE-2020-4200</b>	<a href="https://www.ibm.com/support/pages/node/2875251">https://www.ibm.com/support/pages/node/2875251</a>	A-IBM-DB2-050320/114
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-02-2020	7.2	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 is vulnerable to a buffer overflow, caused by improper bounds checking which could allow a local attacker to execute arbitrary code on the system with root privileges. IBM X-Force ID: 174960. <b>CVE ID : CVE-2020-4204</b>	<a href="https://www.ibm.com/support/pages/node/2875875">https://www.ibm.com/support/pages/node/2875875</a>	A-IBM-DB2-050320/115

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	19-02-2020	4.6	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.1 and 11.5 is vulnerable to an escalation of privilege when an authenticated local attacker with special permissions executes specially crafted Db2 commands. IBM X-Force ID: 175212. <b>CVE ID : CVE-2020-4230</b>	<a href="https://www.ibm.com/support/pages/node/2878809">https://www.ibm.com/support/pages/node/2878809</a>	A-IBM-DB2-050320/116
<b>spectrum_protect</b>					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	24-02-2020	10	IBM Spectrum Protect Plus 10.1.0 and 10.1.5 could allow a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. IBM X-Force ID: 175020. <b>CVE ID : CVE-2020-4210</b>	<a href="https://www.ibm.com/support/pages/node/3178863">https://www.ibm.com/support/pages/node/3178863</a>	A-IBM-SPEC-050320/117
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	24-02-2020	10	IBM Spectrum Protect Plus 10.1.0 and 10.1.5 could allow a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. IBM X-Force ID: 175022. <b>CVE ID : CVE-2020-4211</b>	<a href="https://www.ibm.com/support/pages/node/3178863">https://www.ibm.com/support/pages/node/3178863</a>	A-IBM-SPEC-050320/118
Improper Neutralization	24-02-2020	10	IBM Spectrum Protect Plus 10.1.0 and 10.1.5 could allow	<a href="https://www.ibm.com/">https://www.ibm.com/</a>	A-IBM-SPEC-050320/119

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements in Output Used by a Downstream Component ('Injection')			a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. IBM X-Force ID: 175023. <b>CVE ID : CVE-2020-4212</b>	support/pages/node/3178863	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	24-02-2020	10	IBM Spectrum Protect Plus 10.1.0 and 10.1.5 could allow a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. IBM X-Force ID: 175024. <b>CVE ID : CVE-2020-4213</b>	<a href="https://www.ibm.com/support/pages/node/3178863">https://www.ibm.com/support/pages/node/3178863</a>	A-IBM-SPEC-050320/120
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	24-02-2020	10	IBM Spectrum Protect Plus 10.1.0 and 10.1.5 could allow a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. IBM X-Force ID: 175091. <b>CVE ID : CVE-2020-4222</b>	<a href="https://www.ibm.com/support/pages/node/3178863">https://www.ibm.com/support/pages/node/3178863</a>	A-IBM-SPEC-050320/121
<b>icehrm</b>					
<b>icehrm</b>					
Cross-Site Request Forgery	18-02-2020	6.8	ICE Hrm 26.2.0 is vulnerable to CSRF that leads to password reset via	N/A	A-ICE-ICEH-050320/122

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(CSRF)			service.php. <b>CVE ID : CVE-2020-9270</b>		
Cross-Site Request Forgery (CSRF)	18-02-2020	4.3	ICE Hrm 26.2.0 is vulnerable to CSRF that leads to user creation via service.php. <b>CVE ID : CVE-2020-9271</b>	N/A	A-ICE-ICEH-050320/123
<b>Ispconfig</b>					
<b>ispconfig</b>					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-02-2020	9.3	ISPConfig before 3.1.15p3, when the undocumented reverse_proxy_panel_allowed=sites option is manually enabled, allows SQL Injection. <b>CVE ID : CVE-2020-9398</b>	N/A	A-ISP-ISPC-050320/124
<b>Jetbrains</b>					
<b>scala</b>					
Information Exposure	21-02-2020	5	In the JetBrains Scala plugin before 2019.2.1, some artefact dependencies were resolved over unencrypted connections. <b>CVE ID : CVE-2020-7907</b>	N/A	A-JET-SCAL-050320/125
<b>joplin_project</b>					
<b>joplin</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-02-2020	4.3	Joplin through 1.0.184 allows Arbitrary File Read via XSS. <b>CVE ID : CVE-2020-9038</b>	N/A	A-JOP-JOPL-050320/126
<b>iyaml_project</b>					

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<b>jjyaml</b>					
Deserializati on of Untrusted Data	19-02-2020	7.5	JYaml through 1.3 allows remote code execution during deserialization of a malicious payload through the load() function. NOTE: this is a discontinued product.  <b>CVE ID : CVE-2020-8441</b>	N/A	A-JYA-JYAM-050320/127
<b>Kaseya</b>					
<b>traverse</b>					
Improper Neutralizatio n of Special Elements used in an OS Command (OS Command Injection')	17-02-2020	9	Kaseya Traverse before 9.5.20 allows OS command injection attacks against user accounts, associated with a Netflow Top Applications reporting API call. This is exploitable by an authenticated attacker who submits a modified JSON field within POST data.  <b>CVE ID : CVE-2020-8427</b>	<a href="https://helpdesk.kaseya.com/hc/en-gb/articles/360005409538-Traverse-9-5-20-13-February-2020">https://helpdesk.kaseya.com/hc/en-gb/articles/360005409538-Traverse-9-5-20-13-February-2020</a>	A-KAS-TRAV-050320/128
<b>labvantage</b>					
<b>labvantage</b>					
Information Exposure	17-02-2020	5	LabVantage LIMS 8.3 does not properly maintain the confidentiality of database names. For example, the web application exposes the database name. An attacker might be able to enumerate database names by providing his own database name in a request, because the response will return an 'Unrecognized Database exception message if the database does not exist.	N/A	A-LAB-LABV-050320/129

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-7959</b>		
<b>Libarchive</b>					
<b>libarchive</b>					
Improper Input Validation	20-02-2020	6.8	archive_read_support_format_rar5.c in libarchive before 3.4.2 attempts to unpack a RAR5 file with an invalid or corrupted header (such as a header size of zero), leading to a SIGSEGV or possibly unspecified other impact. <b>CVE ID : CVE-2020-9308</b>	N/A	A-LIB-LIBA-050320/130
<b>Litecart</b>					
<b>litecart</b>					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	25-02-2020	6	LiteCart through 2.2.1 allows CSV injection via a customer's profile. <b>CVE ID : CVE-2020-9017</b>	N/A	A-LIT-LITE-050320/131
Cross-Site Request Forgery (CSRF)	25-02-2020	5	LiteCart through 2.2.1 allows admin/?app=users&doc=edit_user CSRF to add a user. <b>CVE ID : CVE-2020-9018</b>	N/A	A-LIT-LITE-050320/132
<b>lua-openssl_project</b>					
<b>lua-openssl</b>					
Improper Certificate Validation	27-02-2020	6.4	openssl_x509_check_host in lua-openssl 0.7.7-1 mishandles X.509 certificate validation because it uses lua_pushboolean for certain non-boolean return values. <b>CVE ID : CVE-2020-9432</b>	N/A	A-LUA-LUA--050320/133

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Certificate Validation	27-02-2020	6.4	openssl_x509_check_email in lua-openssl 0.7.7-1 mishandles X.509 certificate validation because it uses lua_pushboolean for certain non-boolean return values. <b>CVE ID : CVE-2020-9433</b>	N/A	A-LUA-LUA--050320/134
Improper Certificate Validation	27-02-2020	6.4	openssl_x509_check_ip_asc in lua-openssl 0.7.7-1 mishandles X.509 certificate validation because it uses lua_pushboolean for certain non-boolean return values. <b>CVE ID : CVE-2020-9434</b>	N/A	A-LUA-LUA--050320/135
<b>machothemes</b>					
<b>modula_image_gallery</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-02-2020	3.5	A stored XSS vulnerability exists in the Modula Image Gallery plugin before 2.2.5 for WordPress. Successful exploitation of this vulnerability would allow an authenticated low-privileged user to inject arbitrary JavaScript code that is viewed by other users. <b>CVE ID : CVE-2020-9003</b>	N/A	A-MAC-MODU-050320/136
<b>McAfee</b>					
<b>data_exchange_layer</b>					
Unquoted Search Path or Element	17-02-2020	1.9	Unquoted service executable path in DXL Broker in McAfee Data eXchange Layer (DXL) Framework 6.0.0 and earlier allows local users to cause a denial of service and malicious file execution via carefully crafted and named executable files.	<a href="https://kc.mcafee.com/corporate/index?page=content&amp;id=SB10307">https://kc.mcafee.com/corporate/index?page=content&amp;id=SB10307</a>	A-MCA-DATA-050320/137

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-7252</b>		
<b>miniorange</b>					
<b>saml_sp_single_sign_on</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-02-2020	4.3	Utilities.php in the miniorange-saml-20-single-sign-on plugin before 4.8.84 for WordPress allows XSS via a crafted SAML XML Response to wp-login.php. This is related to the SAMLResponse and RelayState variables, and the Destination parameter of the samlp:Response XML element. <b>CVE ID : CVE-2020-6850</b>	N/A	A-MIN-SAML-050320/138
<b>Mitel</b>					
<b>micontact_center_business</b>					
Incorrect Authorization	25-02-2020	4	The Software Development Kit of the MiContact Center Business with Site Based Security 8.0 through 9.0.1.0 before KB496276 allows an authenticated user to access sensitive information. A successful exploit could allow unauthorized access to user conversations. <b>CVE ID : CVE-2020-9379</b>	<a href="https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-20-0003">https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-20-0003</a>	A-MIT-MICO-050320/139
<b>Moodle</b>					
<b>moodle</b>					
Information Exposure	17-02-2020	4	Moodle before version 3.7.2 is vulnerable to information exposure of service tokens for users enrolled in the same course. <b>CVE ID : CVE-2020-1692</b>	<a href="https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1692">https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1692</a>	A-MOO-MOOD-050320/140

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<b>Mozilla</b>					
<b>webthings_gateway</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-02-2020	4.3	A reflected XSS vulnerability exists within the gateway, allowing an attacker to craft a specialized URL which could steal the user's authentication token. When combined with CVE-2020-6803, an attacker could fully compromise the system. <b>CVE ID : CVE-2020-6804</b>	N/A	A-MOZ-WEBT-050320/141
<b>networkmanager-ssh_project</b>					
<b>networkmanager-ssh</b>					
Improper Privilege Management	23-02-2020	7.5	danfruehauf NetworkManager-ssh before 1.2.11 allows privilege escalation because extra options are mishandled. <b>CVE ID : CVE-2020-9355</b>	N/A	A-NET-NETW-050320/142
<b>openfortivpn_project</b>					
<b>openfortivpn</b>					
Improper Certificate Validation	27-02-2020	5	An issue was discovered in openfortivpn 1.11.0 when used with OpenSSL 1.0.2 or later. tunnel.c mishandles certificate validation because an X509_check_host negative error code is interpreted as a successful return value. <b>CVE ID : CVE-2020-7041</b>	N/A	A-OPE-OPEN-050320/143
Improper Certificate Validation	27-02-2020	5	An issue was discovered in openfortivpn 1.11.0 when used with OpenSSL 1.0.2 or later. tunnel.c mishandles certificate validation	N/A	A-OPE-OPEN-050320/144

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			because the hostname check operates on uninitialized memory. The outcome is that a valid certificate is never accepted (only a malformed certificate may be accepted). <b>CVE ID : CVE-2020-7042</b>		
Improper Certificate Validation	27-02-2020	6.4	An issue was discovered in openfortivpn 1.11.0 when used with OpenSSL before 1.0.2. tunnel.c mishandles certificate validation because hostname comparisons do not consider '\0' characters, as demonstrated by a good.example.com\x00evil.example.com attack. <b>CVE ID : CVE-2020-7043</b>	N/A	A-OPE-OPEN-050320/145
<b>openhab</b>					
<b>openhab</b>					
Incorrect Authorization	20-02-2020	9.3	openHAB before 2.5.2 allow a remote attacker to use REST calls to install the EXEC binding or EXEC transformation service and execute arbitrary commands on the system with the privileges of the user running openHAB. Starting with version 2.5.2 all commands need to be whitelisted in a local file which cannot be changed via REST calls. <b>CVE ID : CVE-2020-5242</b>	<a href="https://github.com/openhab/openhab-addons/security/advisories/GHSA-w698-693g-23hv">https://github.com/openhab/openhab-addons/security/advisories/GHSA-w698-693g-23hv</a>	A-OPE-OPEN-050320/146
<b>opensmtpd</b>					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<b>opensmtpd</b>					
Time-of-check Time-of-use (TOCTOU) Race Condition	25-02-2020	4.7	OpenSMTPD before 6.6.4 allows local users to read arbitrary files (e.g., on some Linux distributions) because of a combination of an untrusted search path in makemap.c and race conditions in the offline functionality in smtpd.c. <b>CVE ID : CVE-2020-8793</b>	N/A	A-OPE-OPEN-050320/147
Out-of-bounds Read	25-02-2020	10	OpenSMTPD before 6.6.4 allows remote code execution because of an out-of-bounds read in mta_io in mta_session.c for multi-line replies. Although this vulnerability affects the client side of OpenSMTPD, it is possible to attack a server because the server code launches the client code during bounce handling. <b>CVE ID : CVE-2020-8794</b>	N/A	A-OPE-OPEN-050320/148
<b>Openssl</b>					
<b>openssl</b>					
Improper Certificate Validation	27-02-2020	5	An issue was discovered in openfortivpn 1.11.0 when used with OpenSSL 1.0.2 or later. tunnel.c mishandles certificate validation because an X509_check_host negative error code is interpreted as a successful return value. <b>CVE ID : CVE-2020-7041</b>	N/A	A-OPE-OPEN-050320/149
Improper Certificate	27-02-2020	5	An issue was discovered in openfortivpn 1.11.0 when	N/A	A-OPE-OPEN-050320/150

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			used with OpenSSL 1.0.2 or later. tunnel.c mishandles certificate validation because the hostname check operates on uninitialized memory. The outcome is that a valid certificate is never accepted (only a malformed certificate may be accepted). <b>CVE ID : CVE-2020-7042</b>		
Improper Certificate Validation	27-02-2020	6.4	An issue was discovered in openfortivpn 1.11.0 when used with OpenSSL before 1.0.2. tunnel.c mishandles certificate validation because hostname comparisons do not consider '\0' characters, as demonstrated by a good.example.com\x00evil.example.com attack. <b>CVE ID : CVE-2020-7043</b>	N/A	A-OPE-OPEN-050320/151
<b>Openvpn</b>					
<b>connect</b>					
Improper Preservation of Permissions	28-02-2020	7.2	OpenVPN Connect 3.1.0.361 on Windows has Insecure Permissions for %PROGRAMDATA%\OpenVPN Connect\drivers\tap\amd64\win10, which allows local users to gain privileges by copying a malicious drvstore.dll there. <b>CVE ID : CVE-2020-9442</b>	N/A	A-OPE-CONN-050320/152
<b>pdf-image_project</b>					
<b>pdf-image</b>					

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	28-02-2020	7.5	Lack of input validation in pdf-image npm package version <= 2.0.0 may allow an attacker to run arbitrary code if PDF file path is constructed based on untrusted user input. <b>CVE ID : CVE-2020-8132</b>	N/A	A-PDF-PDF--050320/153
<b>PHP</b>					
<b>php</b>					
Out-of-bounds Read	27-02-2020	6.4	In PHP versions 7.3.x below 7.3.15 and 7.4.x below 7.4.3, while extracting PHAR files on Windows using phar extension, certain content inside PHAR file could lead to one-byte read past the allocated buffer. This could potentially lead to information disclosure or crash. <b>CVE ID : CVE-2020-7061</b>	N/A	A-PHP-PHP-050320/154
NULL Pointer Dereference	27-02-2020	4.3	In PHP versions 7.2.x below 7.2.28, 7.3.x below 7.3.15 and 7.4.x below 7.4.3, when using file upload functionality, if upload progress tracking is enabled, but session.upload_progress.cleanup is set to 0 (disabled), and the file upload fails, the upload procedure would try to clean up data that does not exist and encounter null pointer dereference, which would likely lead to a crash. <b>CVE ID : CVE-2020-7062</b>	N/A	A-PHP-PHP-050320/155

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Preservation of Permissions	27-02-2020	5	In PHP versions 7.2.x below 7.2.28, 7.3.x below 7.3.15 and 7.4.x below 7.4.3, when creating PHAR archive using PharData::buildFromIterator () function, the files are added with default permissions (0666, or all access) even if the original files on the filesystem were with more restrictive permissions. This may result in files having more lax permissions than intended when such archive is extracted.  <b>CVE ID : CVE-2020-7063</b>	N/A	A-PHP-PHP-050320/156
<b>Proftpd</b>					
<b>proftpd</b>					
Out-of-bounds Read	20-02-2020	5	ProFTPD 1.3.7 has an out-of-bounds (OOB) read vulnerability in mod_cap via the cap_text.c cap_to_text function.  <b>CVE ID : CVE-2020-9272</b>	<a href="https://github.com/proftpd/proftpd/blob/master/RELEASE_NOTES">https://github.com/proftpd/proftpd/blob/master/RELEASE_NOTES</a> , <a href="https://github.com/proftpd/proftpd/issues/902">https://github.com/proftpd/proftpd/issues/902</a>	A-PRO-PROF-050320/157
Use After Free	20-02-2020	9	In ProFTPD 1.3.7, it is possible to corrupt the memory pool by interrupting the data transfer channel. This triggers a use-after-free in alloc_pool in pool.c, and possible remote code execution.	<a href="https://github.com/proftpd/proftpd/blob/master/RELEASE_NOTES">https://github.com/proftpd/proftpd/blob/master/RELEASE_NOTES</a> , <a href="https://github.com/proftpd/proftpd/issues/902">https://github.com/proftpd/proftpd/issues/902</a>	A-PRO-PROF-050320/158

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-9273</b>	3	
<b>Puppet</b>					
<b>puppet_agent</b>					
Improper Certificate Validation	19-02-2020	4	<p>Previously, Puppet operated on a model that a node with a valid certificate was entitled to all information in the system and that a compromised certificate allowed access to everything in the infrastructure. When a node's catalog falls back to the `default` node, the catalog can be retrieved for a different node by modifying facts for the Puppet run. This issue can be mitigated by setting `strict_hostname_checking = true` in `puppet.conf` on your Puppet master. Puppet 6.13.0 changes the default behavior for strict_hostname_checking from false to true. It is recommended that Puppet Open Source and Puppet Enterprise users that are not upgrading still set strict_hostname_checking to true to ensure secure behavior.</p> <p><b>CVE ID : CVE-2020-7942</b></p>	<a href="https://puppet.com/security/cve/CVE-2020-7942/">https://puppet.com/security/cve/CVE-2020-7942/</a>	A-PUP-PUPP-050320/159
<b>puppet</b>					
Improper Certificate Validation	19-02-2020	4	<p>Previously, Puppet operated on a model that a node with a valid certificate was entitled to all information in the system and that a</p>	<a href="https://puppet.com/security/cve/CVE-2020-7942/">https://puppet.com/security/cve/CVE-2020-7942/</a>	A-PUP-PUPP-050320/160

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>compromised certificate allowed access to everything in the infrastructure. When a node's catalog falls back to the `default` node, the catalog can be retrieved for a different node by modifying facts for the Puppet run. This issue can be mitigated by setting `strict_hostname_checking = true` in `puppet.conf` on your Puppet master. Puppet 6.13.0 changes the default behavior for `strict_hostname_checking` from false to true. It is recommended that Puppet Open Source and Puppet Enterprise users that are not upgrading still set `strict_hostname_checking` to true to ensure secure behavior.</p> <p><b>CVE ID : CVE-2020-7942</b></p>		
<b>Pureftpd</b>					
<b>pure-ftpd</b>					
Out-of-bounds Read	24-02-2020	5	<p>An issue was discovered in Pure-FTPd 1.0.49. An out-of-bounds (OOB) read has been detected in the pure_strcmp function in utils.c.</p> <p><b>CVE ID : CVE-2020-9365</b></p>	N/A	A-PUR-PURE-050320/161
<b>realestateconnected</b>					
<b>easy_property_listings</b>					
Cross-Site Request Forgery	18-02-2020	6.8	<p>Cross-site request forgery (CSRF) vulnerability in Easy Property Listings versions prior to 3.4 allows remote</p>	N/A	A-REA-EASY-050320/162

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(CSRF)			attackers to hijack the authentication of administrators via unspecified vectors. <b>CVE ID : CVE-2020-5530</b>		
<b>red-gate</b>					
<b>sql_monitor</b>					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-02-2020	6.5	Red Gate SQL Monitor 9.0.13 through 9.2.14 allows an administrative user to perform a SQL injection attack by configuring the SNMP alert settings in the UI. This is fixed in 9.2.15. <b>CVE ID : CVE-2020-9318</b>	N/A	A-RED-SQL_-050320/163
<b>Redhat</b>					
<b>openshift_service_mesh</b>					
Improper Privilege Management	17-02-2020	4.6	An insecure modification vulnerability in the /etc/passwd file was found in all versions of OpenShift ServiceMesh (maistra) before 1.0.8 in the openshift/istio-kialia-rhel7-operator-container. An attacker with access to the container could use this flaw to modify /etc/passwd and escalate their privileges. <b>CVE ID : CVE-2020-1704</b>	<a href="https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1704">https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1704</a>	A-RED-OPEN-050320/164
<b>spacewalk</b>					
Improper Restriction of XML External Entity Reference	17-02-2020	7.5	A flaw was found in Spacewalk up to version 2.9 where it was vulnerable to XML internal entity attacks via the /rpc/api endpoint. An unauthenticated remote	<a href="https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1693">https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1693</a>	A-RED-SPAC-050320/165

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('XXE')			attacker could use this flaw to retrieve the content of certain files and trigger a denial of service, or in certain circumstances, execute arbitrary code on the Spacewalk server. <b>CVE ID : CVE-2020-1693</b>		
<b>revealjs</b>					
<b>reveal.js</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-02-2020	4.3	Insufficient validation in cross-origin communication (postMessage) in reveal.js version 3.9.1 and earlier allow attackers to perform cross-site scripting attacks. <b>CVE ID : CVE-2020-8127</b>	N/A	A-REV-REVE-050320/166
<b>Ruby-lang</b>					
<b>rake</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-02-2020	9.3	There is an OS command injection vulnerability in Ruby Rake < 12.3.3 in Rake::FileList when supplying a filename that begins with the pipe character ` `. <b>CVE ID : CVE-2020-8130</b>	N/A	A-RUB-RAKE-050320/167
<b>SAS</b>					
<b>visual_analytics</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site	23-02-2020	3.5	Graph Builder in SAS Visual Analytics 8.5 allows XSS via a graph template that is accessed directly. <b>CVE ID : CVE-2020-9350</b>	N/A	A-SAS-VISU-050320/168

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')					
<b>smartclient</b>					
<b>smartclient</b>					
Information Exposure	23-02-2020	5	An issue was discovered in SmartClient 12.0. If an unauthenticated attacker makes a POST request to /tools/developerConsoleOperations.jsp or /isomorphic/IDACall with malformed XML data in the _transaction parameter, the server replies with a verbose error showing where the application resides (the absolute path). <b>CVE ID : CVE-2020-9351</b>	N/A	A-SMA-SMAR-050320/169
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	23-02-2020	7.5	An issue was discovered in SmartClient 12.0. Unauthenticated exploitation of blind XXE can occur in the downloadWSDL feature by sending a POST request to /tools/developerConsoleOperations.jsp with a valid payload in the _transaction parameter. <b>CVE ID : CVE-2020-9352</b>	N/A	A-SMA-SMAR-050320/170
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-02-2020	5	An issue was discovered in SmartClient 12.0. The Remote Procedure Call (RPC) loadFile provided by the console functionality on the /tools/developerConsoleOperations.jsp (or /isomorphic/IDACall) URL is affected by unauthenticated	N/A	A-SMA-SMAR-050320/171

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Local File Inclusion via directory-traversal sequences in the elem XML element in the _transaction parameter. <b>CVE ID : CVE-2020-9353</b>		
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	23-02-2020	6.4	An issue was discovered in SmartClient 12.0. The Remote Procedure Call (RPC) saveFile provided by the console functionality on the /tools/developerConsoleOperations.jsp (or /isomorphic/IDACall) URL allows an unauthenticated attacker to overwrite files via vectors involving an XML comment and ../ path traversal. <b>CVE ID : CVE-2020-9354</b>	N/A	A-SMA-SMAR-050320/172
<b>soplanning</b>					
<b>soplanning</b>					
Cross-Site Request Forgery (CSRF)	18-02-2020	4.3	SOPlanning 1.45 is vulnerable to a CSRF attack that allows for arbitrary changing of the admin password via process/xajax_server.php. <b>CVE ID : CVE-2020-9266</b>	N/A	A-SOP-SOPL-050320/173
Cross-Site Request Forgery (CSRF)	18-02-2020	4.3	SOPlanning 1.45 is vulnerable to a CSRF attack that allows for arbitrary user creation via process/xajax_server.php. <b>CVE ID : CVE-2020-9267</b>	N/A	A-SOP-SOPL-050320/174
Improper Neutralization	18-02-2020	5	SoPlanning 1.45 is vulnerable to SQL Injection	N/A	A-SOP-SOPL-050320/175

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in an SQL Command ('SQL Injection')			in the OrderBy clause, as demonstrated by the projets.php?order=nom_crateur&by= substring. <b>CVE ID : CVE-2020-9268</b>		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-02-2020	9	SOPlanning 1.45 is vulnerable to authenticated SQL Injection that leads to command execution via the users parameter, as demonstrated by export_ical.php. <b>CVE ID : CVE-2020-9269</b>	N/A	A-SOP-SOPL-050320/176
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-02-2020	3.5	SOPlanning 1.45 allows XSS via the "Your SoPlanning url" field. <b>CVE ID : CVE-2020-9338</b>	N/A	A-SOP-SOPL-050320/177
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-02-2020	3.5	SOPlanning 1.45 allows XSS via the Name or Comment to status.php. <b>CVE ID : CVE-2020-9339</b>	N/A	A-SOP-SOPL-050320/178
<b>Sqlite</b>					
<b>sqlite</b>					
NULL Pointer Dereference	21-02-2020	5	In SQLite 3.31.1, isAuxiliaryVtabOperator allows attackers to trigger a NULL pointer dereference and segmentation fault	N/A	A-SQL-SQLI-050320/179

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			because of generated column optimizations. <b>CVE ID : CVE-2020-9327</b>		
<b>supsysic</b>					
<b>pricing_table_by_supsysic</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-02-2020	4.3	An issue was discovered in the pricing-table-by-supsysic plugin before 1.8.2 for WordPress. It allows XSS. <b>CVE ID : CVE-2020-9393</b>	N/A	A-SUP-PRIC-050320/180
Cross-Site Request Forgery (CSRF)	25-02-2020	6.8	An issue was discovered in the pricing-table-by-supsysic plugin before 1.8.2 for WordPress. It allows CSRF. <b>CVE ID : CVE-2020-9394</b>	N/A	A-SUP-PRIC-050320/181
<b>sygnoos</b>					
<b>popup_builder</b>					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-02-2020	7.5	The Popup Builder plugin 2.2.8 through 2.6.7.6 for WordPress is vulnerable to SQL injection (in the sgImportPopups function in sg_popup_ajax.php) via PHP Deserialization on attacker-controlled data with the attachmentUrl POST variable. This allows creation of an arbitrary WordPress Administrator account, leading to possible Remote Code Execution because Administrators can run PHP code on Wordpress instances. (This issue has	N/A	A-SYG-POPU-050320/182

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			been fixed in the 3.x branch of popup-builder.) <b>CVE ID : CVE-2020-9006</b>		
<b>Sympa</b>					
<b>sympa</b>					
Uncontrolled Resource Consumption	24-02-2020	5	Sympa 6.2.38 through 6.2.52 allows remote attackers to cause a denial of service (disk consumption from temporary files, and a flood of notifications to listmasters) via a series of requests with malformed parameters. <b>CVE ID : CVE-2020-9369</b>	N/A	A-SYM-SYMP-050320/183
<b>synacor</b>					
<b>zimbra_collaboration_suite</b>					
Server-Side Request Forgery (SSRF)	18-02-2020	6.8	Zimbra Collaboration Suite (ZCS) before 8.8.15 Patch 7 allows SSRF when WebEx zimlet is installed and zimlet JSP is enabled. <b>CVE ID : CVE-2020-7796</b>	<a href="https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P7">https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P7</a>	A-SYN-ZIMB-050320/184
Improper Preservation of Permissions	18-02-2020	5	An issue was discovered in Zimbra Collaboration Suite (ZCS) before 8.8.15 Patch 7. When grantors revoked a shared calendar in Outlook, the calendar stayed mounted and accessible. <b>CVE ID : CVE-2020-8633</b>	<a href="https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P7">https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P7</a>	A-SYN-ZIMB-050320/185
<b>Topmanage</b>					
<b>olk_webstore</b>					
Cross-Site Request Forgery	18-02-2020	6.8	In TopManage OLK 2020, login CSRF can be chained with another vulnerability in order to takeover admin and	N/A	A-TOP-OLK_-050320/186

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(CSRF)			user accounts. <b>CVE ID : CVE-2020-6844</b>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-02-2020	4.3	An issue was discovered in TopManage OLK 2020. As there is no ReadOnly on the Session cookie, the user and admin accounts can be taken over in a DOM-Based XSS attack. <b>CVE ID : CVE-2020-6845</b>	N/A	A-TOP-OLK_-050320/187
<b>totaljs</b>					
<b>total.js_cms</b>					
Exposure of Resource to Wrong Sphere	24-02-2020	5	controllers/admin.js in Total.js CMS 13 allows remote attackers to execute arbitrary code via a POST to the /admin/api/widgets/ URI. This can be exploited in conjunction with CVE-2019-15954. <b>CVE ID : CVE-2020-9381</b>	N/A	A-TOT-TOTA-050320/188
<b>Trendmicro</b>					
<b>vulnerability_protection</b>					
Uncontrolled Search Path Element	20-02-2020	4.6	Trend Micro Vulnerability Protection 2.0 is affected by a vulnerability that could allow an attack to use the product installer to load other DLL files located in the same directory. <b>CVE ID : CVE-2020-8601</b>	N/A	A-TRE-VULN-050320/189
<b>uap-core_project</b>					
<b>uap-core</b>					
Uncontrolled Resource Consumption	21-02-2020	5	uap-core before 0.7.3 is vulnerable to a denial of service attack when processing crafted User-	<a href="https://github.com/uaparser/uap-core/security">https://github.com/uaparser/uap-core/security</a>	A-UAP-UAP--050320/190

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Agent strings. Some regexes are vulnerable to regular expression denial of service (REDoS) due to overlapping capture groups. This allows remote attackers to overload a server by setting the User-Agent header in an HTTP(S) request to maliciously crafted long strings. This has been patched in uap-core 0.7.3. <b>CVE ID : CVE-2020-5243</b>	ty/advisories/GHSA-cmcx-xhr8-3w9p	
<b>Valve</b>					
<b>dota_2</b>					
Improper Input Validation	17-02-2020	6.8	meshsystem.dll in Valve Dota 2 through 2020-02-17 allows remote attackers to achieve code execution or denial of service by creating a gaming server with a crafted map, and inviting a victim to this server. A GetValue call is mishandled. <b>CVE ID : CVE-2020-9005</b>	N/A	A-VAL-DOTA-050320/191
<b>Vmware</b>					
<b>vrealize_operations</b>					
Improper Input Validation	19-02-2020	7.5	vRealize Operations for Horizon Adapter (6.7.x prior to 6.7.1 and 6.6.x prior to 6.6.1) uses a JMX RMI service which is not securely configured. An unauthenticated remote attacker who has network access to vRealize Operations, with the Horizon Adapter running, may be able to execute arbitrary	<a href="https://www.vmware.com/security/advisories/VMSA-2020-0003.html">https://www.vmware.com/security/advisories/VMSA-2020-0003.html</a>	A-VMW-VREA-050320/192

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code in vRealize Operations. <b>CVE ID : CVE-2020-3943</b>		
Improper Authentication	19-02-2020	5	vRealize Operations for Horizon Adapter (6.7.x prior to 6.7.1 and 6.6.x prior to 6.6.1) has an improper trust store configuration leading to authentication bypass. An unauthenticated remote attacker who has network access to vRealize Operations, with the Horizon Adapter running, may be able to bypass Adapter authentication. <b>CVE ID : CVE-2020-3944</b>	<a href="https://www.vmware.com/security/advisories/VMSA-2020-0003.html">https://www.vmware.com/security/advisories/VMSA-2020-0003.html</a>	A-VMW-VREA-050320/193
Information Exposure	19-02-2020	5	vRealize Operations for Horizon Adapter (6.7.x prior to 6.7.1 and 6.6.x prior to 6.6.1) contains an information disclosure vulnerability due to incorrect pairing implementation between the vRealize Operations for Horizon Adapter and Horizon View. An unauthenticated remote attacker who has network access to vRealize Operations, with the Horizon Adapter running, may obtain sensitive information <b>CVE ID : CVE-2020-3945</b>	<a href="https://www.vmware.com/security/advisories/VMSA-2020-0003.html">https://www.vmware.com/security/advisories/VMSA-2020-0003.html</a>	A-VMW-VREA-050320/194
<b>webnus</b>					
<b>modern_events_calendar_lite</b>					
Improper Neutralization of Input	28-02-2020	3.5	Multiple Stored Cross-site scripting (XSS) vulnerabilities in the	N/A	A-WEB-MODE-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Webnus Modern Events Calendar Lite plugin through 5.1.6 for WordPress allows remote authenticated users (with minimal permissions) to inject arbitrary JavaScript, HTML, or CSS via Ajax actions. This affects mec_save_notifications and import_settings. <b>CVE ID : CVE-2020-9459</b>		050320/195
<b>western_digital</b>					
<b>ibi</b>					
Session Fixation	20-02-2020	6.4	Western Digital My Cloud Home before 3.6.0 and ibi before 3.6.0 allow Session Fixation. <b>CVE ID : CVE-2020-8990</b>	N/A	A-WES-IBI-050320/196
<b>my_cloud_home</b>					
Session Fixation	20-02-2020	6.4	Western Digital My Cloud Home before 3.6.0 and ibi before 3.6.0 allow Session Fixation. <b>CVE ID : CVE-2020-8990</b>	N/A	A-WES-MY_C-050320/197
<b>westerndigital</b>					
<b>sandiskssddashboardsetup.exe</b>					
Uncontrolled Search Path Element	19-02-2020	4.4	Western Digital WesternDigitalSSDDashboardSetup.exe before 3.0.2.0 allows DLL Hijacking. <b>CVE ID : CVE-2020-8959</b>	N/A	A-WES-SAND-050320/198
<b>westerndigitalssddashboardsetup.exe</b>					
Uncontrolled Search Path Element	19-02-2020	4.4	Western Digital WesternDigitalSSDDashboardSetup.exe before 3.0.2.0 allows DLL Hijacking.	N/A	A-WES-WEST-050320/199

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-8959</b>		
<b>mycloud.com</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-02-2020	4.3	Western Digital mycloud.com before Web Version 2.2.0-134 allows XSS. <b>CVE ID : CVE-2020-8960</b>	N/A	A-WES-MYCL-050320/200
<b>Wireshark</b>					
<b>wireshark</b>					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	27-02-2020	5	In Wireshark 3.2.0 to 3.2.1, 3.0.0 to 3.0.8, and 2.6.0 to 2.6.14, the EAP dissector could crash. This was addressed in epan/dissectors/packet-eap.c by using more careful sscanf parsing. <b>CVE ID : CVE-2020-9428</b>	N/A	A-WIR-WIRE-050320/201
NULL Pointer Dereference	27-02-2020	5	In Wireshark 3.2.0 to 3.2.1, the WireGuard dissector could crash. This was addressed in epan/dissectors/packet-wireguard.c by handling the situation where a certain data structure intentionally has a NULL value. <b>CVE ID : CVE-2020-9429</b>	N/A	A-WIR-WIRE-050320/202
Improper Input Validation	27-02-2020	5	In Wireshark 3.2.0 to 3.2.1, 3.0.0 to 3.0.8, and 2.6.0 to 2.6.14, the WiMax DLMAP dissector could crash. This was addressed in plugins/epan/wimax/msg_d_lmap.c by validating a length	N/A	A-WIR-WIRE-050320/203

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			field. <b>CVE ID : CVE-2020-9430</b>		
Uncontrolled Resource Consumption	27-02-2020	5	In Wireshark 3.2.0 to 3.2.1, 3.0.0 to 3.0.8, and 2.6.0 to 2.6.14, the LTE RRC dissector could leak memory. This was addressed in epan/dissectors/packet-lte-rrc.c by adjusting certain append operations. <b>CVE ID : CVE-2020-9431</b>	N/A	A-WIR-WIRE-050320/204
<b>wpcentral</b>					
<b>wpcentral</b>					
Improper Privilege Management	17-02-2020	9	The wpCentral plugin before 1.5.1 for WordPress allows disclosure of the connection key. <b>CVE ID : CVE-2020-9043</b>	N/A	A-WPC-WPCE-050320/205
<b>wpjobboard</b>					
<b>wpjobboard</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-02-2020	4.3	The WPJobBoard plugin 5.5.3 for WordPress allows Persistent XSS via the Add Job form, as demonstrated by title and Description. <b>CVE ID : CVE-2020-9019</b>	N/A	A-WPJ-WPJO-050320/206
<b>yarnpkg</b>					
<b>yarn</b>					
Improper Limitation of a Pathname to a Restricted Directory ('Path	24-02-2020	7.5	Arbitrary filesystem write vulnerability in Yarn before 1.22.0 allows attackers to write to any path on the filesystem and potentially lead to arbitrary code execution by forcing the user	<a href="https://github.com/yarnpkg/yarn/pull/7831">https://github.com/yarnpkg/yarn/pull/7831</a>	A-YAR-YARN-050320/207

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			to install a malicious package. <b>CVE ID : CVE-2020-8131</b>		
<b>zint</b>					
<b>zint</b>					
NULL Pointer Dereference	25-02-2020	5	A NULL Pointer Dereference exists in libzint in Zint 2.7.1 because multiple + characters are mishandled in add_on in upcean.c, when called from eanx in upcean.c during EAN barcode generation. <b>CVE ID : CVE-2020-9385</b>	N/A	A-ZIN-ZINT-050320/208
<b>Hardware</b>					
<b>abbott</b>					
<b>freestyle_libre</b>					
Out-of-bounds Write	16-02-2020	5.8	Older generation Abbott FreeStyle Libre sensors allow remote attackers within close proximity to enable write access to memory via a specific NFC unlock command. NOTE: The vulnerability is not present in the FreeStyle Libre 14-day in the U.S (announced in August 2018) and FreeStyle Libre 2 outside the U.S (announced in October 2018). <b>CVE ID : CVE-2020-8997</b>	N/A	H-ABB-FREE-050320/209
<b>cambiumnetworks</b>					
<b>xh2-120</b>					
Improper Neutralization of Input	17-02-2020	4.3	An issue was discovered on Xirrus XR520, XR620, XR2436, and XH2-120	N/A	H-CAM-XH2--050320/210

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			devices. The cgi-bin/ViewPage.cgi user parameter allows XSS. <b>CVE ID : CVE-2020-9022</b>		
<b>xr2436</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-02-2020	4.3	An issue was discovered on Xirrus XR520, XR620, XR2436, and XH2-120 devices. The cgi-bin/ViewPage.cgi user parameter allows XSS. <b>CVE ID : CVE-2020-9022</b>	N/A	H-CAM-XR24-050320/211
<b>xr520</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-02-2020	4.3	An issue was discovered on Xirrus XR520, XR620, XR2436, and XH2-120 devices. The cgi-bin/ViewPage.cgi user parameter allows XSS. <b>CVE ID : CVE-2020-9022</b>	N/A	H-CAM-XR52-050320/212
<b>xr620</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-02-2020	4.3	An issue was discovered on Xirrus XR520, XR620, XR2436, and XH2-120 devices. The cgi-bin/ViewPage.cgi user parameter allows XSS. <b>CVE ID : CVE-2020-9022</b>	N/A	H-CAM-XR62-050320/213
<b>Cisco</b>					
<b>nexus_31128pq</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated,	N/A	H-CIS-NEXU-050320/214

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>		
<b>nexus_3132c-z</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a</p>	N/A	H-CIS-NEXU-050320/215

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions. <b>CVE ID : CVE-2020-3174</b>		
<b>nexus_3132q</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions. <b>CVE ID : CVE-2020-3174</b>	N/A	H-CIS-NEXU-050320/216

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<b>nexus_3132q-v</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>	N/A	H-CIS-NEXU-050320/217
<b>nexus_3132q-xl</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to</p>	N/A	H-CIS-NEXU-050320/218

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>		
<b>nexus_3164q</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with</p>	N/A	H-CIS-NEXU-050320/219

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			incorrect entries, which could lead to traffic disruptions. <b>CVE ID : CVE-2020-3174</b>		
<b>nexus_3172</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions. <b>CVE ID : CVE-2020-3174</b>	N/A	H-CIS-NEXU-050320/220
<b>nexus_3172pq-xl</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid	N/A	H-CIS-NEXU-050320/221

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>		
<b>nexus_3172tq</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the</p>	N/A	H-CIS-NEXU-050320/222

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>		
<b>nexus_3172tq-32t</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>	N/A	H-CIS-NEXU-050320/223
<b>nexus_3172tq-xl</b>					
Insufficient	26-02-2020	3.3	A vulnerability in the	N/A	H-CIS-NEXU-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Verification of Data Authenticity			<p>anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>		050320/224
<b>nexus_3264c-e</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP</p>	N/A	H-CIS-NEXU-050320/225

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>(GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>		
<b>nexus_3264q</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic</p>	N/A	H-CIS-NEXU-050320/226

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disruptions. <b>CVE ID : CVE-2020-3174</b>		
<b>nexus_3408-s</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions. <b>CVE ID : CVE-2020-3174</b>	N/A	H-CIS-NEXU-050320/227
<b>nexus_34180yc</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP	N/A	H-CIS-NEXU-050320/228

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>		
<b>nexus_3432d-s</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A</p>	N/A	H-CIS-NEXU-050320/229

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions. <b>CVE ID : CVE-2020-3174</b>		
<b>nexus_3464c</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions. <b>CVE ID : CVE-2020-3174</b>	N/A	H-CIS-NEXU-050320/230
<b>nexus_3524</b>					
Insufficient Verification of Data	26-02-2020	3.3	A vulnerability in the anycast gateway feature of Cisco NX-OS Software could	N/A	H-CIS-NEXU-050320/231

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authenticity			<p>allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>		
<b>nexus_3524-x</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this</p>	N/A	H-CIS-NEXU-050320/232

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>		
<b>nexus_3524-xl</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>	N/A	H-CIS-NEXU-050320/233

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<b>nexus_3548</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>	N/A	H-CIS-NEXU-050320/234
<b>nexus_3548-x</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to</p>	N/A	H-CIS-NEXU-050320/235

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>		
<b>nexus_3548-xl</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with</p>	N/A	H-CIS-NEXU-050320/236

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			incorrect entries, which could lead to traffic disruptions. <b>CVE ID : CVE-2020-3174</b>		
<b>nexus_36180yc-r</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions. <b>CVE ID : CVE-2020-3174</b>	N/A	H-CIS-NEXU-050320/237
<b>nexus_3636c-r</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid	N/A	H-CIS-NEXU-050320/238

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>		
<b>nexus_7000</b>					
Improper Input Validation	26-02-2020	4.3	<p>A vulnerability in the NX-API feature of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause an NX-API system process to unexpectedly restart. The vulnerability is due to incorrect validation of the HTTP header of a request that is sent to the NX-API. An attacker could exploit this vulnerability by sending a crafted HTTP request to the NX-API on an affected device. A successful exploit could allow the attacker to cause a denial of service</p>	N/A	H-CIS-NEXU-050320/239

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(DoS) condition in the NX-API service; however, the Cisco NX-OS device itself would still be available and passing network traffic. Note: The NX-API feature is disabled by default. <b>CVE ID : CVE-2020-3170</b>		
Insufficient Verification of Data Authenticity	26-02-2020	3.3	A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions. <b>CVE ID : CVE-2020-3174</b>	N/A	H-CIS-NEXU-050320/240
<b>nexus_7700</b>					
Improper Input Validation	26-02-2020	4.3	A vulnerability in the NX-API feature of Cisco NX-OS Software could allow an unauthenticated, remote	N/A	H-CIS-NEXU-050320/241

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker to cause an NX-API system process to unexpectedly restart. The vulnerability is due to incorrect validation of the HTTP header of a request that is sent to the NX-API. An attacker could exploit this vulnerability by sending a crafted HTTP request to the NX-API on an affected device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition in the NX-API service; however, the Cisco NX-OS device itself would still be available and passing network traffic. Note: The NX-API feature is disabled by default.</p> <p><b>CVE ID : CVE-2020-3170</b></p>		
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to</p>	N/A	H-CIS-NEXU-050320/242

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions. <b>CVE ID : CVE-2020-3174</b>		
<b>firepower_9300</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	A vulnerability in the CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS). The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges. <b>CVE ID : CVE-2020-3167</b>	N/A	H-CIS-FIRE-050320/243
Improper Neutralization of Special	26-02-2020	7.2	A vulnerability in the local management (local-mgmt) CLI of Cisco FXOS Software	N/A	H-CIS-FIRE-050320/244

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) of an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges. <b>CVE ID : CVE-2020-3171</b>		
<b>firepower_4115</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	A vulnerability in the CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS). The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by	N/A	H-CIS-FIRE-050320/245

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges. <b>CVE ID : CVE-2020-3167</b>		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying Linux operating system with a privilege level of root on an affected device. The vulnerability is due to insufficient validation of arguments passed to a specific CLI command on the affected device. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system with root privileges. An attacker would need valid administrator	N/A	H-CIS-FIRE-050320/246

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials to exploit this vulnerability. <b>CVE ID : CVE-2020-3169</b>		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	A vulnerability in the local management (local-mgmt) CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) of an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges. <b>CVE ID : CVE-2020-3171</b>	N/A	H-CIS-FIRE-050320/247
<b>firepower_4125</b>					
Improper Neutralization of Special Elements used in an OS Command	26-02-2020	7.2	A vulnerability in the CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary	N/A	H-CIS-FIRE-050320/248

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			<p>commands on the underlying operating system (OS). The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges.</p> <p><b>CVE ID : CVE-2020-3167</b></p>		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	<p>A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying Linux operating system with a privilege level of root on an affected device. The vulnerability is due to insufficient validation of arguments passed to a specific CLI command on the affected device. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the</p>	N/A	H-CIS-FIRE-050320/249

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary commands on the underlying Linux operating system with root privileges. An attacker would need valid administrator credentials to exploit this vulnerability. <b>CVE ID : CVE-2020-3169</b>		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	A vulnerability in the local management (local-mgmt) CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) of an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges. <b>CVE ID : CVE-2020-3171</b>	N/A	H-CIS-FIRE-050320/250
firepower_4145					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	<p>A vulnerability in the CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS). The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges.</p> <p><b>CVE ID : CVE-2020-3167</b></p>	N/A	H-CIS-FIRE-050320/251
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	<p>A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying Linux operating system with a privilege level of root on an affected device. The vulnerability is due to insufficient validation of arguments passed to a specific CLI command on the affected device. An attacker</p>	N/A	H-CIS-FIRE-050320/252

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system with root privileges. An attacker would need valid administrator credentials to exploit this vulnerability.</p> <p><b>CVE ID : CVE-2020-3169</b></p>		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	<p>A vulnerability in the local management (local-mgmt) CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) of an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric</p>	N/A	H-CIS-FIRE-050320/253

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Interconnects, the injected commands are executed with root privileges. <b>CVE ID : CVE-2020-3171</b>		
<b>firepower_4110</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	A vulnerability in the CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS). The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges. <b>CVE ID : CVE-2020-3167</b>	N/A	H-CIS-FIRE-050320/254
Improper Neutralization of Special Elements used in an OS Command ('OS	26-02-2020	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying Linux operating system with a privilege level	N/A	H-CIS-FIRE-050320/255

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			<p>of root on an affected device. The vulnerability is due to insufficient validation of arguments passed to a specific CLI command on the affected device. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system with root privileges. An attacker would need valid administrator credentials to exploit this vulnerability.</p> <p><b>CVE ID : CVE-2020-3169</b></p>		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	<p>A vulnerability in the local management (local-mgmt) CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) of an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the</p>	N/A	H-CIS-FIRE-050320/256

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges.</p> <p><b>CVE ID : CVE-2020-3171</b></p>		
<b>firepower_4120</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	<p>A vulnerability in the CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS). The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges.</p> <p><b>CVE ID : CVE-2020-3167</b></p>	N/A	H-CIS-FIRE-050320/257

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	<p>A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying Linux operating system with a privilege level of root on an affected device. The vulnerability is due to insufficient validation of arguments passed to a specific CLI command on the affected device. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system with root privileges. An attacker would need valid administrator credentials to exploit this vulnerability.</p> <p><b>CVE ID : CVE-2020-3169</b></p>	N/A	H-CIS-FIRE-050320/258
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	<p>A vulnerability in the local management (local-mgmt) CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) of an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit</p>	N/A	H-CIS-FIRE-050320/259

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges.</p> <p><b>CVE ID : CVE-2020-3171</b></p>		
<b>firepower_4140</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	<p>A vulnerability in the CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS). The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric</p>	N/A	H-CIS-FIRE-050320/260

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges. <b>CVE ID : CVE-2020-3167</b>		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying Linux operating system with a privilege level of root on an affected device. The vulnerability is due to insufficient validation of arguments passed to a specific CLI command on the affected device. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system with root privileges. An attacker would need valid administrator credentials to exploit this vulnerability. <b>CVE ID : CVE-2020-3169</b>	N/A	H-CIS-FIRE-050320/261
Improper Neutralization of Special Elements used in an OS Command	26-02-2020	7.2	A vulnerability in the local management (local-mgmt) CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker	N/A	H-CIS-FIRE-050320/262

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			to execute arbitrary commands on the underlying operating system (OS) of an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges. <b>CVE ID : CVE-2020-3171</b>		
<b>firepower_4150</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	A vulnerability in the CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS). The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could	N/A	H-CIS-FIRE-050320/263

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges. <b>CVE ID : CVE-2020-3167</b>		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying Linux operating system with a privilege level of root on an affected device. The vulnerability is due to insufficient validation of arguments passed to a specific CLI command on the affected device. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system with root privileges. An attacker would need valid administrator credentials to exploit this vulnerability.	N/A	H-CIS-FIRE-050320/264

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-3169</b>		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	<p>A vulnerability in the local management (local-mgmt) CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) of an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges.</p> <p><b>CVE ID : CVE-2020-3171</b></p>	N/A	H-CIS-FIRE-050320/265
<b>firepower_1010</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	<p>A vulnerability in the CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system</p>	N/A	H-CIS-FIRE-050320/266

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			(OS). The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges. <b>CVE ID : CVE-2020-3167</b>		
<b>firepower_1120</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	A vulnerability in the CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS). The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently	N/A	H-CIS-FIRE-050320/267

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges. <b>CVE ID : CVE-2020-3167</b>		
<b>firepower_1140</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	A vulnerability in the CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS). The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges. <b>CVE ID : CVE-2020-3167</b>	N/A	H-CIS-FIRE-050320/268
<b>firepower_2110</b>					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	<p>A vulnerability in the CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS). The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges.</p> <p><b>CVE ID : CVE-2020-3167</b></p>	N/A	H-CIS-FIRE-050320/269
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	<p>A vulnerability in the local management (local-mgmt) CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) of an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit</p>	N/A	H-CIS-FIRE-050320/270

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges.</p> <p><b>CVE ID : CVE-2020-3171</b></p>		
<b>firepower_2120</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	<p>A vulnerability in the CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS). The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric</p>	N/A	H-CIS-FIRE-050320/271

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges. <b>CVE ID : CVE-2020-3167</b>		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	A vulnerability in the local management (local-mgmt) CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) of an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges. <b>CVE ID : CVE-2020-3171</b>	N/A	H-CIS-FIRE-050320/272
<b>firepower_2130</b>					
Improper Neutralization of Special	26-02-2020	7.2	A vulnerability in the CLI of Cisco FXOS Software and Cisco UCS Manager Software	N/A	H-CIS-FIRE-050320/273

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS). The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges.  <b>CVE ID : CVE-2020-3167</b>		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	A vulnerability in the local management (local-mgmt) CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) of an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A	N/A	H-CIS-FIRE-050320/274

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges. <b>CVE ID : CVE-2020-3171</b>		
<b>firepower_2140</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	A vulnerability in the CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS). The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected	N/A	H-CIS-FIRE-050320/275

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			commands are executed with root privileges. <b>CVE ID : CVE-2020-3167</b>		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	A vulnerability in the local management (local-mgmt) CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) of an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges. <b>CVE ID : CVE-2020-3171</b>	N/A	H-CIS-FIRE-050320/276
<b>ucs_6248up</b>					
Improper Neutralization of Special Elements used in an OS Command	26-02-2020	7.2	A vulnerability in the CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary	N/A	H-CIS-UCS_-050320/277

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			<p>commands on the underlying operating system (OS). The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges.</p> <p><b>CVE ID : CVE-2020-3167</b></p>		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	<p>A vulnerability in the local management (local-mgmt) CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) of an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the</p>	N/A	H-CIS-UCS_-050320/278

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges. <b>CVE ID : CVE-2020-3171</b>		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	A vulnerability in the local management (local-mgmt) CLI of Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) on an affected device. The vulnerability is due to insufficient input validation of command arguments. An attacker could exploit this vulnerability by including crafted arguments to specific commands on the local management CLI. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed	N/A	H-CIS-UCS_-050320/279

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with root privileges. <b>CVE ID : CVE-2020-3173</b>		
<b>ucs_6296up</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	A vulnerability in the CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS). The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges. <b>CVE ID : CVE-2020-3167</b>	N/A	H-CIS-UCS_-050320/280
Improper Neutralization of Special Elements used in an OS Command ('OS Command	26-02-2020	7.2	A vulnerability in the local management (local-mgmt) CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system	N/A	H-CIS-UCS_-050320/281

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			<p>(OS) of an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges.</p> <p><b>CVE ID : CVE-2020-3171</b></p>		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	<p>A vulnerability in the local management (local-mgmt) CLI of Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) on an affected device. The vulnerability is due to insufficient input validation of command arguments. An attacker could exploit this vulnerability by including crafted arguments to specific commands on the local management CLI. A successful exploit could allow the attacker to execute arbitrary commands on the</p>	N/A	H-CIS-UCS_-050320/282

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges. <b>CVE ID : CVE-2020-3173</b>		
<b>ucs_6332</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	A vulnerability in the CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS). The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges. <b>CVE ID : CVE-2020-3167</b>	N/A	H-CIS-UCS_-050320/283

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	<p>A vulnerability in the local management (local-mgmt) CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) of an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges.</p> <p><b>CVE ID : CVE-2020-3171</b></p>	N/A	H-CIS-UCS_-050320/284
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	<p>A vulnerability in the local management (local-mgmt) CLI of Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) on an affected device. The vulnerability is due to insufficient input validation</p>	N/A	H-CIS-UCS_-050320/285

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>of command arguments. An attacker could exploit this vulnerability by including crafted arguments to specific commands on the local management CLI. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges.</p> <p><b>CVE ID : CVE-2020-3173</b></p>		
<b>mds_9132t</b>					
Improper Input Validation	26-02-2020	4.3	<p>A vulnerability in the NX-API feature of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause an NX-API system process to unexpectedly restart. The vulnerability is due to incorrect validation of the HTTP header of a request that is sent to the NX-API. An attacker could exploit this vulnerability by sending a crafted HTTP request to the NX-API on an affected device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition in the NX-</p>	N/A	H-CIS-MDS_-050320/286

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			API service; however, the Cisco NX-OS device itself would still be available and passing network traffic. Note: The NX-API feature is disabled by default. <b>CVE ID : CVE-2020-3170</b>		
Insufficient Verification of Data Authenticity	26-02-2020	3.3	A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions. <b>CVE ID : CVE-2020-3174</b>	N/A	H-CIS-MDS_-050320/287
Uncontrolled Resource Consumption	26-02-2020	7.8	A vulnerability in the resource handling system of Cisco NX-OS Software for Cisco MDS 9000 Series Multilayer Switches could allow an unauthenticated,	N/A	H-CIS-MDS_-050320/288

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper resource usage control. An attacker could exploit this vulnerability by sending traffic to the management interface (mgmt0) of an affected device at very high rates. An exploit could allow the attacker to cause unexpected behaviors such as high CPU usage, process crashes, or even full system reboots of an affected device. <b>CVE ID : CVE-2020-3175</b>		
<b>mds_9148s</b>					
Improper Input Validation	26-02-2020	4.3	A vulnerability in the NX-API feature of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause an NX-API system process to unexpectedly restart. The vulnerability is due to incorrect validation of the HTTP header of a request that is sent to the NX-API. An attacker could exploit this vulnerability by sending a crafted HTTP request to the NX-API on an affected device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition in the NX-API service; however, the Cisco NX-OS device itself	N/A	H-CIS-MDS_-050320/289

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			would still be available and passing network traffic. Note: The NX-API feature is disabled by default. <b>CVE ID : CVE-2020-3170</b>		
Insufficient Verification of Data Authenticity	26-02-2020	3.3	A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions. <b>CVE ID : CVE-2020-3174</b>	N/A	H-CIS-MDS_-050320/290
Uncontrolled Resource Consumption	26-02-2020	7.8	A vulnerability in the resource handling system of Cisco NX-OS Software for Cisco MDS 9000 Series Multilayer Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	N/A	H-CIS-MDS_-050320/291

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			condition on an affected device. The vulnerability is due to improper resource usage control. An attacker could exploit this vulnerability by sending traffic to the management interface (mgmt0) of an affected device at very high rates. An exploit could allow the attacker to cause unexpected behaviors such as high CPU usage, process crashes, or even full system reboots of an affected device. <b>CVE ID : CVE-2020-3175</b>		
<b>mds_9148t</b>					
Improper Input Validation	26-02-2020	4.3	A vulnerability in the NX-API feature of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause an NX-API system process to unexpectedly restart. The vulnerability is due to incorrect validation of the HTTP header of a request that is sent to the NX-API. An attacker could exploit this vulnerability by sending a crafted HTTP request to the NX-API on an affected device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition in the NX-API service; however, the Cisco NX-OS device itself would still be available and passing network traffic.	N/A	H-CIS-MDS_-050320/292

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Note: The NX-API feature is disabled by default. <b>CVE ID : CVE-2020-3170</b>		
Insufficient Verification of Data Authenticity	26-02-2020	3.3	A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions. <b>CVE ID : CVE-2020-3174</b>	N/A	H-CIS-MDS_-050320/293
Uncontrolled Resource Consumption	26-02-2020	7.8	A vulnerability in the resource handling system of Cisco NX-OS Software for Cisco MDS 9000 Series Multilayer Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is	N/A	H-CIS-MDS_-050320/294

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>due to improper resource usage control. An attacker could exploit this vulnerability by sending traffic to the management interface (mgmt0) of an affected device at very high rates. An exploit could allow the attacker to cause unexpected behaviors such as high CPU usage, process crashes, or even full system reboots of an affected device.</p> <p><b>CVE ID : CVE-2020-3175</b></p>		
<b>mds_9216</b>					
Improper Input Validation	26-02-2020	4.3	<p>A vulnerability in the NX-API feature of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause an NX-API system process to unexpectedly restart. The vulnerability is due to incorrect validation of the HTTP header of a request that is sent to the NX-API. An attacker could exploit this vulnerability by sending a crafted HTTP request to the NX-API on an affected device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition in the NX-API service; however, the Cisco NX-OS device itself would still be available and passing network traffic. Note: The NX-API feature is disabled by default.</p>	N/A	H-CIS-MDS_-050320/295

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-3170</b>		
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>	N/A	H-CIS-MDS_-050320/296
Uncontrolled Resource Consumption	26-02-2020	7.8	<p>A vulnerability in the resource handling system of Cisco NX-OS Software for Cisco MDS 9000 Series Multilayer Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper resource usage control. An attacker</p>	N/A	H-CIS-MDS_-050320/297

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending traffic to the management interface (mgmt0) of an affected device at very high rates. An exploit could allow the attacker to cause unexpected behaviors such as high CPU usage, process crashes, or even full system reboots of an affected device. <b>CVE ID : CVE-2020-3175</b>		
<b>mds_9216a</b>					
Improper Input Validation	26-02-2020	4.3	A vulnerability in the NX-API feature of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause an NX-API system process to unexpectedly restart. The vulnerability is due to incorrect validation of the HTTP header of a request that is sent to the NX-API. An attacker could exploit this vulnerability by sending a crafted HTTP request to the NX-API on an affected device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition in the NX-API service; however, the Cisco NX-OS device itself would still be available and passing network traffic. Note: The NX-API feature is disabled by default. <b>CVE ID : CVE-2020-3170</b>	N/A	H-CIS-MDS_-050320/298

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>	N/A	H-CIS-MDS_-050320/299
Uncontrolled Resource Consumption	26-02-2020	7.8	<p>A vulnerability in the resource handling system of Cisco NX-OS Software for Cisco MDS 9000 Series Multilayer Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper resource usage control. An attacker could exploit this vulnerability by sending</p>	N/A	H-CIS-MDS_-050320/300

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>traffic to the management interface (mgmt0) of an affected device at very high rates. An exploit could allow the attacker to cause unexpected behaviors such as high CPU usage, process crashes, or even full system reboots of an affected device.</p> <p><b>CVE ID : CVE-2020-3175</b></p>		
<b>mds_9216i</b>					
Improper Input Validation	26-02-2020	4.3	<p>A vulnerability in the NX-API feature of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause an NX-API system process to unexpectedly restart. The vulnerability is due to incorrect validation of the HTTP header of a request that is sent to the NX-API. An attacker could exploit this vulnerability by sending a crafted HTTP request to the NX-API on an affected device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition in the NX-API service; however, the Cisco NX-OS device itself would still be available and passing network traffic. Note: The NX-API feature is disabled by default.</p> <p><b>CVE ID : CVE-2020-3170</b></p>	N/A	H-CIS-MDS_-050320/301
Insufficient Verification of Data	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could</p>	N/A	H-CIS-MDS_-050320/302

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authenticity			<p>allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>		
Uncontrolled Resource Consumption	26-02-2020	7.8	<p>A vulnerability in the resource handling system of Cisco NX-OS Software for Cisco MDS 9000 Series Multilayer Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper resource usage control. An attacker could exploit this vulnerability by sending traffic to the management interface (mgmt0) of an affected device at very high</p>	N/A	H-CIS-MDS_-050320/303

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>rates. An exploit could allow the attacker to cause unexpected behaviors such as high CPU usage, process crashes, or even full system reboots of an affected device.</p> <p><b>CVE ID : CVE-2020-3175</b></p>		
<b>mds_9222i</b>					
Improper Input Validation	26-02-2020	4.3	<p>A vulnerability in the NX-API feature of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause an NX-API system process to unexpectedly restart. The vulnerability is due to incorrect validation of the HTTP header of a request that is sent to the NX-API. An attacker could exploit this vulnerability by sending a crafted HTTP request to the NX-API on an affected device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition in the NX-API service; however, the Cisco NX-OS device itself would still be available and passing network traffic. Note: The NX-API feature is disabled by default.</p> <p><b>CVE ID : CVE-2020-3170</b></p>	N/A	H-CIS-MDS_-050320/304
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid</p>	N/A	H-CIS-MDS_-050320/305

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>		
Uncontrolled Resource Consumption	26-02-2020	7.8	<p>A vulnerability in the resource handling system of Cisco NX-OS Software for Cisco MDS 9000 Series Multilayer Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper resource usage control. An attacker could exploit this vulnerability by sending traffic to the management interface (mgmt0) of an affected device at very high rates. An exploit could allow the attacker to cause unexpected behaviors such</p>	N/A	H-CIS-MDS_-050320/306

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			as high CPU usage, process crashes, or even full system reboots of an affected device. <b>CVE ID : CVE-2020-3175</b>		
<b>mds_9506</b>					
Improper Input Validation	26-02-2020	4.3	A vulnerability in the NX-API feature of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause an NX-API system process to unexpectedly restart. The vulnerability is due to incorrect validation of the HTTP header of a request that is sent to the NX-API. An attacker could exploit this vulnerability by sending a crafted HTTP request to the NX-API on an affected device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition in the NX-API service; however, the Cisco NX-OS device itself would still be available and passing network traffic. Note: The NX-API feature is disabled by default. <b>CVE ID : CVE-2020-3170</b>	N/A	H-CIS-MDS_-050320/307
Insufficient Verification of Data Authenticity	26-02-2020	3.3	A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP	N/A	H-CIS-MDS_-050320/308

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions. <b>CVE ID : CVE-2020-3174</b>		
Uncontrolled Resource Consumption	26-02-2020	7.8	A vulnerability in the resource handling system of Cisco NX-OS Software for Cisco MDS 9000 Series Multilayer Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper resource usage control. An attacker could exploit this vulnerability by sending traffic to the management interface (mgmt0) of an affected device at very high rates. An exploit could allow the attacker to cause unexpected behaviors such as high CPU usage, process crashes, or even full system	N/A	H-CIS-MDS_-050320/309

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reboots of an affected device. <b>CVE ID : CVE-2020-3175</b>		
<b>mds_9509</b>					
Improper Input Validation	26-02-2020	4.3	A vulnerability in the NX-API feature of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause an NX-API system process to unexpectedly restart. The vulnerability is due to incorrect validation of the HTTP header of a request that is sent to the NX-API. An attacker could exploit this vulnerability by sending a crafted HTTP request to the NX-API on an affected device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition in the NX-API service; however, the Cisco NX-OS device itself would still be available and passing network traffic. Note: The NX-API feature is disabled by default. <b>CVE ID : CVE-2020-3170</b>	N/A	H-CIS-MDS_-050320/310
Insufficient Verification of Data Authenticity	26-02-2020	3.3	A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to	N/A	H-CIS-MDS_-050320/311

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>		
Uncontrolled Resource Consumption	26-02-2020	7.8	<p>A vulnerability in the resource handling system of Cisco NX-OS Software for Cisco MDS 9000 Series Multilayer Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper resource usage control. An attacker could exploit this vulnerability by sending traffic to the management interface (mgmt0) of an affected device at very high rates. An exploit could allow the attacker to cause unexpected behaviors such as high CPU usage, process crashes, or even full system reboots of an affected device.</p> <p><b>CVE ID : CVE-2020-3175</b></p>	N/A	H-CIS-MDS_-050320/312

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<b>mds_9513</b>					
Improper Input Validation	26-02-2020	4.3	<p>A vulnerability in the NX-API feature of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause an NX-API system process to unexpectedly restart. The vulnerability is due to incorrect validation of the HTTP header of a request that is sent to the NX-API. An attacker could exploit this vulnerability by sending a crafted HTTP request to the NX-API on an affected device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition in the NX-API service; however, the Cisco NX-OS device itself would still be available and passing network traffic. Note: The NX-API feature is disabled by default.</p> <p><b>CVE ID : CVE-2020-3170</b></p>	N/A	H-CIS-MDS_-050320/313
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP</p>	N/A	H-CIS-MDS_-050320/314

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>(GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>		
Uncontrolled Resource Consumption	26-02-2020	7.8	<p>A vulnerability in the resource handling system of Cisco NX-OS Software for Cisco MDS 9000 Series Multilayer Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper resource usage control. An attacker could exploit this vulnerability by sending traffic to the management interface (mgmt0) of an affected device at very high rates. An exploit could allow the attacker to cause unexpected behaviors such as high CPU usage, process crashes, or even full system reboots of an affected device.</p> <p><b>CVE ID : CVE-2020-3175</b></p>	N/A	H-CIS-MDS_-050320/315
mds_9706					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	26-02-2020	4.3	<p>A vulnerability in the NX-API feature of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause an NX-API system process to unexpectedly restart. The vulnerability is due to incorrect validation of the HTTP header of a request that is sent to the NX-API. An attacker could exploit this vulnerability by sending a crafted HTTP request to the NX-API on an affected device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition in the NX-API service; however, the Cisco NX-OS device itself would still be available and passing network traffic. Note: The NX-API feature is disabled by default.</p> <p><b>CVE ID : CVE-2020-3170</b></p>	N/A	H-CIS-MDS_-050320/316
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this</p>	N/A	H-CIS-MDS_-050320/317

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>		
Uncontrolled Resource Consumption	26-02-2020	7.8	<p>A vulnerability in the resource handling system of Cisco NX-OS Software for Cisco MDS 9000 Series Multilayer Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper resource usage control. An attacker could exploit this vulnerability by sending traffic to the management interface (mgmt0) of an affected device at very high rates. An exploit could allow the attacker to cause unexpected behaviors such as high CPU usage, process crashes, or even full system reboots of an affected device.</p> <p><b>CVE ID : CVE-2020-3175</b></p>	N/A	H-CIS-MDS_-050320/318
<b>mds_9710</b>					
Improper Input	26-02-2020	4.3	<p>A vulnerability in the NX-API feature of Cisco NX-OS Software could allow an</p>	N/A	H-CIS-MDS_-050320/319

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			<p>unauthenticated, remote attacker to cause an NX-API system process to unexpectedly restart. The vulnerability is due to incorrect validation of the HTTP header of a request that is sent to the NX-API. An attacker could exploit this vulnerability by sending a crafted HTTP request to the NX-API on an affected device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition in the NX-API service; however, the Cisco NX-OS device itself would still be available and passing network traffic. Note: The NX-API feature is disabled by default.</p> <p><b>CVE ID : CVE-2020-3170</b></p>		
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the</p>	N/A	H-CIS-MDS_-050320/320

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions. <b>CVE ID : CVE-2020-3174</b>		
Uncontrolled Resource Consumption	26-02-2020	7.8	A vulnerability in the resource handling system of Cisco NX-OS Software for Cisco MDS 9000 Series Multilayer Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper resource usage control. An attacker could exploit this vulnerability by sending traffic to the management interface (mgmt0) of an affected device at very high rates. An exploit could allow the attacker to cause unexpected behaviors such as high CPU usage, process crashes, or even full system reboots of an affected device. <b>CVE ID : CVE-2020-3175</b>	N/A	H-CIS-MDS_-050320/321
<b>mds_9718</b>					
Improper Input Validation	26-02-2020	4.3	A vulnerability in the NX-API feature of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause an NX-API system process to	N/A	H-CIS-MDS_-050320/322

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>unexpectedly restart. The vulnerability is due to incorrect validation of the HTTP header of a request that is sent to the NX-API. An attacker could exploit this vulnerability by sending a crafted HTTP request to the NX-API on an affected device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition in the NX-API service; however, the Cisco NX-OS device itself would still be available and passing network traffic. Note: The NX-API feature is disabled by default.</p> <p><b>CVE ID : CVE-2020-3170</b></p>		
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could</p>	N/A	H-CIS-MDS_-050320/323

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions. <b>CVE ID : CVE-2020-3174</b>		
Uncontrolled Resource Consumption	26-02-2020	7.8	A vulnerability in the resource handling system of Cisco NX-OS Software for Cisco MDS 9000 Series Multilayer Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper resource usage control. An attacker could exploit this vulnerability by sending traffic to the management interface (mgmt0) of an affected device at very high rates. An exploit could allow the attacker to cause unexpected behaviors such as high CPU usage, process crashes, or even full system reboots of an affected device. <b>CVE ID : CVE-2020-3175</b>	N/A	H-CIS-MDS_-050320/324
<b>ucs_6324</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command	26-02-2020	7.2	A vulnerability in the CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS). The vulnerability is due	N/A	H-CIS-UCS_-050320/325

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			<p>to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges.</p> <p><b>CVE ID : CVE-2020-3167</b></p>		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	<p>A vulnerability in the local management (local-mgmt) CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) of an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all</p>	N/A	H-CIS-UCS_-050320/326

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges. <b>CVE ID : CVE-2020-3171</b>		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	A vulnerability in the local management (local-mgmt) CLI of Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) on an affected device. The vulnerability is due to insufficient input validation of command arguments. An attacker could exploit this vulnerability by including crafted arguments to specific commands on the local management CLI. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges. <b>CVE ID : CVE-2020-3173</b>	N/A	H-CIS-UCS_-050320/327
<b>ucs_6332-16up</b>					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	<p>A vulnerability in the CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS). The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges.</p> <p><b>CVE ID : CVE-2020-3167</b></p>	N/A	H-CIS-UCS_-050320/328
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	<p>A vulnerability in the local management (local-mgmt) CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) of an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit</p>	N/A	H-CIS-UCS_-050320/329

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges.</p> <p><b>CVE ID : CVE-2020-3171</b></p>		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	<p>A vulnerability in the local management (local-mgmt) CLI of Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) on an affected device. The vulnerability is due to insufficient input validation of command arguments. An attacker could exploit this vulnerability by including crafted arguments to specific commands on the local management CLI. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding</p>	N/A	H-CIS-UCS_-050320/330

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges. <b>CVE ID : CVE-2020-3173</b>		
<b>firepower_1150</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	A vulnerability in the CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS). The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges. <b>CVE ID : CVE-2020-3167</b>	N/A	H-CIS-FIRE-050320/331
<b>nexus_3232c_</b>					
Insufficient Verification	26-02-2020	3.3	A vulnerability in the anycast gateway feature of	N/A	H-CIS-NEXU-050320/332

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Data Authenticity			<p>Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>		
<b>ucs_64108</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	<p>A vulnerability in the CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS). The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A</p>	N/A	H-CIS-UCS_-050320/333

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges.</p> <p><b>CVE ID : CVE-2020-3167</b></p>		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	<p>A vulnerability in the local management (local-mgmt) CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) of an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected</p>	N/A	H-CIS-UCS_-050320/334

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			commands are executed with root privileges. <b>CVE ID : CVE-2020-3171</b>		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	A vulnerability in the local management (local-mgmt) CLI of Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) on an affected device. The vulnerability is due to insufficient input validation of command arguments. An attacker could exploit this vulnerability by including crafted arguments to specific commands on the local management CLI. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges. <b>CVE ID : CVE-2020-3173</b>	N/A	H-CIS-UCS_-050320/335
<b>ucs_6454</b>					
Improper Neutralization of Special Elements used in an OS	26-02-2020	7.2	A vulnerability in the CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker	N/A	H-CIS-UCS_-050320/336

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			to execute arbitrary commands on the underlying operating system (OS). The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges. <b>CVE ID : CVE-2020-3167</b>		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	A vulnerability in the local management (local-mgmt) CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) of an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute	N/A	H-CIS-UCS_-050320/337

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges. <b>CVE ID : CVE-2020-3171</b>		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	A vulnerability in the local management (local-mgmt) CLI of Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) on an affected device. The vulnerability is due to insufficient input validation of command arguments. An attacker could exploit this vulnerability by including crafted arguments to specific commands on the local management CLI. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed	N/A	H-CIS-UCS_-050320/338

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with root privileges. <b>CVE ID : CVE-2020-3173</b>		
<b>firepower_9300_sm-24</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying Linux operating system with a privilege level of root on an affected device. The vulnerability is due to insufficient validation of arguments passed to a specific CLI command on the affected device. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system with root privileges. An attacker would need valid administrator credentials to exploit this vulnerability. <b>CVE ID : CVE-2020-3169</b>	N/A	H-CIS-FIRE-050320/339
<b>firepower_9300_sm-36</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS	26-02-2020	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying Linux operating system with a privilege level	N/A	H-CIS-FIRE-050320/340

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			<p>of root on an affected device. The vulnerability is due to insufficient validation of arguments passed to a specific CLI command on the affected device. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system with root privileges. An attacker would need valid administrator credentials to exploit this vulnerability.</p> <p><b>CVE ID : CVE-2020-3169</b></p>		
<b>firepower_9300_sm-40</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	<p>A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying Linux operating system with a privilege level of root on an affected device. The vulnerability is due to insufficient validation of arguments passed to a specific CLI command on the affected device. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful</p>	N/A	H-CIS-FIRE-050320/341

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system with root privileges. An attacker would need valid administrator credentials to exploit this vulnerability.</p> <p><b>CVE ID : CVE-2020-3169</b></p>		
<b>firepower_9300_sm-44</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	<p>A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying Linux operating system with a privilege level of root on an affected device. The vulnerability is due to insufficient validation of arguments passed to a specific CLI command on the affected device. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system with root privileges. An attacker would need valid administrator credentials to exploit this vulnerability.</p> <p><b>CVE ID : CVE-2020-3169</b></p>	N/A	H-CIS-FIRE-050320/342

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<b>firepower_9300_sm-44_x_3</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	<p>A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying Linux operating system with a privilege level of root on an affected device. The vulnerability is due to insufficient validation of arguments passed to a specific CLI command on the affected device. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system with root privileges. An attacker would need valid administrator credentials to exploit this vulnerability.</p> <p><b>CVE ID : CVE-2020-3169</b></p>	N/A	H-CIS-FIRE-050320/343
<b>firepower_9300_sm-48</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	<p>A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying Linux operating system with a privilege level of root on an affected device. The vulnerability is due to insufficient validation of</p>	N/A	H-CIS-FIRE-050320/344

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arguments passed to a specific CLI command on the affected device. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system with root privileges. An attacker would need valid administrator credentials to exploit this vulnerability. <b>CVE ID : CVE-2020-3169</b>		
<b>firepower_9300_sm-56</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying Linux operating system with a privilege level of root on an affected device. The vulnerability is due to insufficient validation of arguments passed to a specific CLI command on the affected device. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the	N/A	H-CIS-FIRE-050320/345

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			underlying Linux operating system with root privileges. An attacker would need valid administrator credentials to exploit this vulnerability. <b>CVE ID : CVE-2020-3169</b>		
<b>firepower_9300_sm-56_x_3</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying Linux operating system with a privilege level of root on an affected device. The vulnerability is due to insufficient validation of arguments passed to a specific CLI command on the affected device. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system with root privileges. An attacker would need valid administrator credentials to exploit this vulnerability. <b>CVE ID : CVE-2020-3169</b>	N/A	H-CIS-FIRE-050320/346
<b>nexus_9000v</b>					
Insufficient Verification	26-02-2020	3.3	A vulnerability in the anycast gateway feature of	N/A	H-CIS-NEXU-050320/347

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Data Authenticity			<p>Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>		
<b>nexus_92160yc-x</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker</p>	N/A	H-CIS-NEXU-050320/348

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>		
<b>nexus_92300yc</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p>	N/A	H-CIS-NEXU-050320/349

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-3174</b>		
<b>nexus_92304qc</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>	N/A	H-CIS-NEXU-050320/350
<b>nexus_92348gc-x</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet.</p>	N/A	H-CIS-NEXU-050320/351

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>		
<b>nexus_9236c</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet.</p> <p>The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to</p>	N/A	H-CIS-NEXU-050320/352

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			populate the ARP table with incorrect entries, which could lead to traffic disruptions. <b>CVE ID : CVE-2020-3174</b>		
<b>nexus_9272q</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions. <b>CVE ID : CVE-2020-3174</b>	N/A	H-CIS-NEXU-050320/353
<b>nexus_93108tc-ex</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a	N/A	H-CIS-NEXU-050320/354

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>		
<b>nexus_93108tc-fx</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on</p>	N/A	H-CIS-NEXU-050320/355

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions. <b>CVE ID : CVE-2020-3174</b>		
<b>nexus_93120tx</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions. <b>CVE ID : CVE-2020-3174</b>	N/A	H-CIS-NEXU-050320/356
<b>nexus_93128tx</b>					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>	N/A	H-CIS-NEXU-050320/357
<b>nexus_93180lc-ex</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a</p>	N/A	H-CIS-NEXU-050320/358

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions. <b>CVE ID : CVE-2020-3174</b>		
<b>nexus_93180yc-ex</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which	N/A	H-CIS-NEXU-050320/359

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could lead to traffic disruptions. <b>CVE ID : CVE-2020-3174</b>		
<b>nexus_93180yc-fx</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions. <b>CVE ID : CVE-2020-3174</b>	N/A	H-CIS-NEXU-050320/360
<b>nexus_93216tc-fx2</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol	N/A	H-CIS-NEXU-050320/361

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>(ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>		
<b>nexus_93240yc-fx2</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to</p>	N/A	H-CIS-NEXU-050320/362

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions. <b>CVE ID : CVE-2020-3174</b>		
<b>nexus_9332c</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions. <b>CVE ID : CVE-2020-3174</b>	N/A	H-CIS-NEXU-050320/363
<b>nexus_9332pq</b>					
Insufficient Verification	26-02-2020	3.3	A vulnerability in the anycast gateway feature of	N/A	H-CIS-NEXU-050320/364

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Data Authenticity			<p>Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>		
<b>nexus_93360yc-fx2</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker</p>	N/A	H-CIS-NEXU-050320/365

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>		
<b>nexus_9336c-fx2</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p>	N/A	H-CIS-NEXU-050320/366

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-3174</b>		
<b>nexus_9336pq_aci_spine</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>	N/A	H-CIS-NEXU-050320/367
<b>nexus_9348gc-fxp</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet.</p>	N/A	H-CIS-NEXU-050320/368

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>		
<b>nexus_9364c</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet.</p> <p>The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to</p>	N/A	H-CIS-NEXU-050320/369

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			populate the ARP table with incorrect entries, which could lead to traffic disruptions. <b>CVE ID : CVE-2020-3174</b>		
<b>nexus_9372px</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions. <b>CVE ID : CVE-2020-3174</b>	N/A	H-CIS-NEXU-050320/370
<b>nexus_9372px-e</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a	N/A	H-CIS-NEXU-050320/371

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>		
<b>nexus_9372tx</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on</p>	N/A	H-CIS-NEXU-050320/372

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions. <b>CVE ID : CVE-2020-3174</b>		
<b>nexus_9372tx-e</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions. <b>CVE ID : CVE-2020-3174</b>	N/A	H-CIS-NEXU-050320/373
<b>nexus_9396px</b>					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>	N/A	H-CIS-NEXU-050320/374
<b>nexus_9396tx</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a</p>	N/A	H-CIS-NEXU-050320/375

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>		
<b>nexus_9504</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which</p>	N/A	H-CIS-NEXU-050320/376

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could lead to traffic disruptions. <b>CVE ID : CVE-2020-3174</b>		
<b>nexus_9508</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions. <b>CVE ID : CVE-2020-3174</b>	N/A	H-CIS-NEXU-050320/377
<b>nexus_9516</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol	N/A	H-CIS-NEXU-050320/378

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>(ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>		
<b>nexus_3016</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to</p>	N/A	H-CIS-NEXU-050320/379

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions. <b>CVE ID : CVE-2020-3174</b>		
<b>nexus_3048</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions. <b>CVE ID : CVE-2020-3174</b>	N/A	H-CIS-NEXU-050320/380
<b>nexus_3064</b>					
Insufficient Verification	26-02-2020	3.3	A vulnerability in the anycast gateway feature of	N/A	H-CIS-NEXU-050320/381

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Data Authenticity			<p>Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>		
<b>nexus_3064-t</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker</p>	N/A	H-CIS-NEXU-050320/382

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.  <b>CVE ID : CVE-2020-3174</b>		
<b>nexus_31108pc-v</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.	N/A	H-CIS-NEXU-050320/383

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-3174</b>		
<b>nexus_31108tc-v</b>					
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>	N/A	H-CIS-NEXU-050320/384
<b>Dell</b>					
<b>g3_15_3590</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an</p>	N/A	H-DEL-G3_1-050320/385

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
<b>g5_15_5590</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	H-DEL-G5_1-050320/386
<b>g5_5090</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File</p>	N/A	H-DEL-G5_5-050320/387

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
<b>g7_15_7590</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	H-DEL-G7_1-050320/388

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<b>g7_17_7790</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	H-DEL-G7_1-050320/389
<b>inspiron_14_5490</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect</p>	N/A	H-DEL-INSP-050320/390

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>		
<b>inspiron_3490</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-INSP-050320/391
<b>inspiron_3493</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit	N/A	H-DEL-INSP-050320/392

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
<b>inspiron_3590</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	H-DEL-INSP-050320/393
<b>inspiron_3593</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window</p>	N/A	H-DEL-INSP-050320/394

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
<b>inspiron_3790</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	H-DEL-INSP-050320/395
<b>inspiron_3793</b>					
Improper Input	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms	N/A	H-DEL-INSP-050320/396

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			<p>contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
<b>inspiron_5390</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p>	N/A	H-DEL-INSP-050320/397

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-5324</b>		
<b>inspiron_5391</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	H-DEL-INSP-050320/398
<b>inspiron_5491</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The</p>	N/A	H-DEL-INSP-050320/399

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>		
<b>inspiron_5493</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-INSP-050320/400
<b>inspiron_5494</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged	N/A	H-DEL-INSP-050320/401

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>		
<b>inspiron_5498</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-INSP-050320/402
<b>inspiron_5583</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility	N/A	H-DEL-INSP-050320/403

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
<b>inspiron_5584</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	H-DEL-INSP-050320/404
<b>inspiron_5590</b>					
Improper	21-02-2020	2.6	Dell Client Consumer and	N/A	H-DEL-INSP-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.  <b>CVE ID : CVE-2020-5324</b>		050320/405
<b>inspiron_5591</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility	N/A	H-DEL-INSP-050320/406

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			delivers. <b>CVE ID : CVE-2020-5324</b>		
<b>inspiron_5593</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-INSP-050320/407
<b>inspiron_5594</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into	N/A	H-DEL-INSP-050320/408

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>		
<b>inspiron_5598</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-INSP-050320/409
<b>inspiron_7390</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this	N/A	H-DEL-INSP-050320/410

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>		
<b>inspiron_7391</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-INSP-050320/411
<b>inspiron_7490</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The	N/A	H-DEL-INSP-050320/412

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
<b>inspiron_7590</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	H-DEL-INSP-050320/413

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-INSP-050320/414
<b>inspiron_7591</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-INSP-050320/415

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-INSP-050320/416
<b>inspiron_7791</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-INSP-050320/417

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<b>latitude_3301</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	H-DEL-LATI-050320/418
<b>latitude_3300</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect</p>	N/A	H-DEL-LATI-050320/419

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>		
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-LATI-050320/420
<b>latitude_3311</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect	N/A	H-DEL-LATI-050320/421

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>		
<b>latitude_3400</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-LATI-050320/422
<b>latitude_3500</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit	N/A	H-DEL-LATI-050320/423

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
<b>latitude_5300</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	H-DEL-LATI-050320/424
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the</p>	N/A	H-DEL-LATI-050320/425

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>latitude_5400</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-LATI-050320/426
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the	N/A	H-DEL-LATI-050320/427

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>latitude_5401</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-LATI-050320/428
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the	N/A	H-DEL-LATI-050320/429

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>latitude_5420_rugged</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-LATI-050320/430
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the	N/A	H-DEL-LATI-050320/431

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>latitude_5424_rugged</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-LATI-050320/432
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the	N/A	H-DEL-LATI-050320/433

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>latitude_5500</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-LATI-050320/434
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the	N/A	H-DEL-LATI-050320/435

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>latitude_5501</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-LATI-050320/436
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the	N/A	H-DEL-LATI-050320/437

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>latitude_7200</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-LATI-050320/438
<b>latitude_7220_rugged_extreme_tablet</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window	N/A	H-DEL-LATI-050320/439

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
<b>latitude_7220ex_rugged_extreme_tablet</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	H-DEL-LATI-050320/440
<b>latitude_7300</b>					
Improper Input	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms	N/A	H-DEL-LATI-050320/441

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			<p>contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	H-DEL-LATI-050320/442
<b>latitude_7400</b>					
Improper Input	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms	N/A	H-DEL-LATI-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			<p>contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		050320/443
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	H-DEL-LATI-050320/444
<b>precision_3540</b>					
Improper Input	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms	N/A	H-DEL-PREC-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			<p>contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		050320/445
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	H-DEL-PREC-050320/446
<b>precision_3541</b>					
Improper Input	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms	N/A	H-DEL-PREC-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.  <b>CVE ID : CVE-2020-5324</b>		050320/447
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.  <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-PREC-050320/448
<b>precision_5540</b>					
Improper Input	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms	N/A	H-DEL-PREC-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			<p>contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		050320/449
<b>precision_7540</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p>	N/A	H-DEL-PREC-050320/450

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-5324</b>		
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-PREC-050320/451
<b>precision_7730</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.	N/A	H-DEL-PREC-050320/452

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-5324</b>		
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	H-DEL-PREC-050320/453
<b>precision_7740</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p>	N/A	H-DEL-PREC-050320/454

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-5324</b>		
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-PREC-050320/455
<b>vostro_15_7580</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.	N/A	H-DEL-VOST-050320/456

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-5324</b>		
<b>vostro_3481</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	H-DEL-VOST-050320/457
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p>	N/A	H-DEL-VOST-050320/458

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-5326</b>		
<b>vostro_3490</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	H-DEL-VOST-050320/459
<b>vostro_3590</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The</p>	N/A	H-DEL-VOST-050320/460

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>		
<b>vostro_5390</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-VOST-050320/461
<b>vostro_5391</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged	N/A	H-DEL-VOST-050320/462

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>		
<b>vostro_5490</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-VOST-050320/463
<b>vostro_5590</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility	N/A	H-DEL-VOST-050320/464

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
<b>vostro_7590</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	H-DEL-VOST-050320/465
Missing Authentication for	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration</p>	N/A	H-DEL-VOST-050320/466

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Critical Function			authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>wyse_5070_thin_client</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-WYSE-050320/467
<b>wyse_5470</b>					
Improper	21-02-2020	2.6	Dell Client Consumer and	N/A	H-DEL-WYSE-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.  <b>CVE ID : CVE-2020-5324</b>		050320/468
<b>xps_13_9380</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility	N/A	H-DEL-XPS_-050320/469

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			delivers. <b>CVE ID : CVE-2020-5324</b>		
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-XPS_-050320/470
<b>xps_15_9575</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility	N/A	H-DEL-XPS_-050320/471

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			delivers. <b>CVE ID : CVE-2020-5324</b>		
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-XPS_-050320/472
<b>xps_15_7590</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility	N/A	H-DEL-XPS_-050320/473

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			delivers. <b>CVE ID : CVE-2020-5324</b>		
<b>xps_15_9570</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-XPS_-050320/474
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-	N/A	H-DEL-XPS_-050320/475

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>g3_3590</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-G3_3-050320/476
<b>inspiron_14_gaming_7466</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.	N/A	H-DEL-INSP-050320/477

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-5326</b>		
<b>inspiron_14_gaming_7467</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	H-DEL-INSP-050320/478
<b>inspiron_15_7572</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	H-DEL-INSP-050320/479

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<b>inspiron_15_gaming_7566</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.  <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-INSP-050320/480
<b>inspiron_15_gaming_7567</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.  <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-INSP-050320/481
<b>g3_3779</b>					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	H-DEL-G3_3-050320/482
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	H-DEL-G3_3-050320/483
latitude_3390					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-LATI-050320/484
latitude_3460					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-LATI-050320/485

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<b>latitude_3480</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.  <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-LATI-050320/486
<b>latitude_3490</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.	N/A	H-DEL-LATI-050320/487

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-5324</b>		
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-LATI-050320/488
latitude_3580					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-LATI-050320/489
latitude_3590					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	H-DEL-LATI-050320/490
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	H-DEL-LATI-050320/491
latitude_5175					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-LATI-050320/492
latitude_5179					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-LATI-050320/493
latitude_5280					
Missing	21-02-2020	2.1	Affected Dell Client	N/A	H-DEL-LATI-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication for Critical Function			platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		050320/494
latitude_5288					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-LATI-050320/495
latitude_5289					
Missing Authentication	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS	N/A	H-DEL-LATI-050320/496

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on for Critical Function			Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
latitude_5290					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-LATI-050320/497
Missing Authenticati	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS	N/A	H-DEL-LATI-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on for Critical Function			Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		050320/498
<b>latitude_5414</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-LATI-050320/499
<b>latitude_5480</b>					
Missing Authentication for	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration	N/A	H-DEL-LATI-050320/500

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Critical Function			authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>latitude_5488</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-LATI-050320/501
<b>latitude_5490</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The	N/A	H-DEL-LATI-050320/502

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	H-DEL-LATI-050320/503
<b>latitude_5491</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The</p>	N/A	H-DEL-LATI-050320/504

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	H-DEL-LATI-050320/505
<b>precision_3620</b>					
Missing Authentication for Critical	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass</p>	N/A	H-DEL-PREC-050320/506

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Function			vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>precision_3630</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-PREC-050320/507
<b>precision_3930</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot	N/A	H-DEL-PREC-050320/508

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>precision_5510</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-PREC-050320/509
<b>precision_5520</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage	N/A	H-DEL-PREC-050320/510

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>precision_5530</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-PREC-050320/511
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage	N/A	H-DEL-PREC-050320/512

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>precision_5820</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-PREC-050320/513
<b>precision_7510</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST)	N/A	H-DEL-PREC-050320/514

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>precision_7520</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-PREC-050320/515
<b>precision_7530</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an	N/A	H-DEL-PREC-050320/516

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	H-DEL-PREC-050320/517
<b>precision_7710</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker</p>	N/A	H-DEL-PREC-050320/518

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>precision_7720</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-PREC-050320/519
<b>precision_7820</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the	N/A	H-DEL-PREC-050320/520

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>precision_7920</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-PREC-050320/521
<b>vostro_7580</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform	N/A	H-DEL-VOST-050320/522

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>vostro_3070</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-VOST-050320/523
<b>chengming_3980</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the	N/A	H-DEL-CHEN-050320/524

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>g7_7790</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-G7_7-050320/525
<b>xps_8900</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration	N/A	H-DEL-XPS_-050320/526

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>g3_3579</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-G3_3-050320/527
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration	N/A	H-DEL-G3_3-050320/528

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>g5_5587</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-G5_5-050320/529
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration	N/A	H-DEL-G5_5-050320/530

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>g5_5590</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-G5_5-050320/531
<b>g7_7588</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking	N/A	H-DEL-G7_7-050320/532

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>		
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-G7_7-050320/533
<b>g7_7590</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring	N/A	H-DEL-G7_7-050320/534

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>embedded_box_pc_5000</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-EMBE-050320/535
<b>latitude_5580</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by	N/A	H-DEL-LATI-050320/536

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>latitude_5590</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-LATI-050320/537
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by	N/A	H-DEL-LATI-050320/538

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>latitude_5591</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-LATI-050320/539
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by	N/A	H-DEL-LATI-050320/540

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>latitude_7202</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-LATI-050320/541
<b>latitude_7212</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized	N/A	H-DEL-LATI-050320/542

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>latitude_7214</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-LATI-050320/543
<b>latitude_7275</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-	N/A	H-DEL-LATI-050320/544

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>latitude_7280</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-LATI-050320/545
<b>latitude_7285</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.	N/A	H-DEL-LATI-050320/546

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-5326</b>		
<b>latitude_7290</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	H-DEL-LATI-050320/547
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p>	N/A	H-DEL-LATI-050320/548

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-5326</b>		
<b>latitude_7370</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-LATI-050320/549
<b>latitude_7380</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-LATI-050320/550

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<b>latitude_7389</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	H-DEL-LATI-050320/551
<b>latitude_7390</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p>	N/A	H-DEL-LATI-050320/552

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-5324</b>		
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-LATI-050320/553
latitude_7414					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-LATI-050320/554
latitude_7424_rugged_extreme					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	H-DEL-LATI-050320/555
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	H-DEL-LATI-050320/556
latitude_7480					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-LATI-050320/557
latitude_7490					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-LATI-050320/558

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-LATI-050320/559
latitude_e5270					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-LATI-050320/560
latitude_e5470					
Missing	21-02-2020	2.1	Affected Dell Client	N/A	H-DEL-LATI-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication for Critical Function			platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		050320/561
latitude_e5570					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-LATI-050320/562
latitude_e7270					
Missing Authentication	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS	N/A	H-DEL-LATI-050320/563

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on for Critical Function			Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>latitude_e7470</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-LATI-050320/564
<b>optiplex_3040</b>					
Missing Authentication for	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration	N/A	H-DEL-OPTI-050320/565

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Critical Function			authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>optiplex_3046</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-OPTI-050320/566
<b>optiplex_3050</b>					
Missing Authentication for Critical	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass	N/A	H-DEL-OPTI-050320/567

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Function			vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>optiplex_3060</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-OPTI-050320/568
<b>optiplex_5040</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot	N/A	H-DEL-OPTI-050320/569

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>optiplex_5060</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-OPTI-050320/570
<b>optiplex_7050</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage	N/A	H-DEL-OPTI-050320/571

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>optiplex_7060</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-OPTI-050320/572
<b>optiplex_xe3</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST)	N/A	H-DEL-OPTI-050320/573

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>precision_3420</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-PREC-050320/574
<b>precision_3430</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker	N/A	H-DEL-PREC-050320/575

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>precision_3510</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-PREC-050320/576
<b>precision_3520</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the	N/A	H-DEL-PREC-050320/577

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>precision_3530</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-PREC-050320/578
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the	N/A	H-DEL-PREC-050320/579

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>inspiron_15_gaming_7577</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-INSP-050320/580
<b>inspiron_3670</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform	N/A	H-DEL-INSP-050320/581

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>inspiron_5488</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-INSP-050320/582
<b>optiplex_3070</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the	N/A	H-DEL-OPTI-050320/583

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>optiplex_3240</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-OPTI-050320/584
<b>optiplex_5070</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration	N/A	H-DEL-OPTI-050320/585

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>optiplex_5250</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-OPTI-050320/586
<b>optiplex_5260</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring	N/A	H-DEL-OPTI-050320/587

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>optiplex_7070</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-OPTI-050320/588
<b>optiplex_7440</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by	N/A	H-DEL-OPTI-050320/589

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>optiplex_7460</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-OPTI-050320/590
<b>optiplex_7760</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized	N/A	H-DEL-OPTI-050320/591

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>optiplex_5270</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-OPTI-050320/592
<b>optiplex_7470</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-	N/A	H-DEL-OPTI-050320/593

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>optiplex_7770</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-OPTI-050320/594
<b>precision_5720</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.	N/A	H-DEL-PREC-050320/595

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-5326</b>		
<b>precision_5810</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-PREC-050320/596
<b>precision_7810</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-PREC-050320/597

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<b>precision_7910</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.  <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-PREC-050320/598
<b>precision_3431</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.  <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-PREC-050320/599
<b>vostro_15_7570</b>					

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-VOST-050320/600
<b>xps_12_9250</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-XPS_-050320/601
<b>xps_13_9343</b>					
Missing	21-02-2020	2.1	Affected Dell Client	N/A	H-DEL-XPS_-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication for Critical Function			platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		050320/602
<b>xps_13_9350</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-XPS_-050320/603
<b>xps_13_9360</b>					
Missing Authentication	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS	N/A	H-DEL-XPS_-050320/604

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on for Critical Function			Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>xps_15_9550</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-XPS_-050320/605
<b>xps_15_9560</b>					
Missing Authentication for	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration	N/A	H-DEL-XPS_-050320/606

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Critical Function			authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>xps_27_7760</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-XPS_-050320/607
<b>inspiron_3470</b>					
Missing Authentication for Critical	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass	N/A	H-DEL-INSP-050320/608

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Function			vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>inspiron_3480</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-INSP-050320/609
Missing Authentication for Critical	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass	N/A	H-DEL-INSP-050320/610

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Function			vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>inspiron_3481</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-INSP-050320/611
Missing Authentication for Critical	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass	N/A	H-DEL-INSP-050320/612

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Function			vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>inspiron_3580</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-INSP-050320/613
Missing Authentication for Critical	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass	N/A	H-DEL-INSP-050320/614

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Function			vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>inspiron_3583</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-INSP-050320/615
Missing Authentication for Critical	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass	N/A	H-DEL-INSP-050320/616

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Function			vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>inspiron_3581</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-INSP-050320/617
Missing Authentication for Critical	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass	N/A	H-DEL-INSP-050320/618

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Function			vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>inspiron_3584</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-INSP-050320/619
Missing Authentication for Critical	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass	N/A	H-DEL-INSP-050320/620

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Function			vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>inspiron_3780</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-INSP-050320/621
Missing Authentication for Critical	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass	N/A	H-DEL-INSP-050320/622

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Function			vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>inspiron_3781</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-INSP-050320/623
Missing Authentication for Critical	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass	N/A	H-DEL-INSP-050320/624

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Function			vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>inspiron_5370</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-INSP-050320/625
<b>inspiron_5480</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the	N/A	H-DEL-INSP-050320/626

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	H-DEL-INSP-050320/627
<b>inspiron_5481</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the</p>	N/A	H-DEL-INSP-050320/628

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	H-DEL-INSP-050320/629
<b>inspiron_5482</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the</p>	N/A	H-DEL-INSP-050320/630

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	H-DEL-INSP-050320/631
<b>inspiron_5570</b>					
Missing Authentication for Critical	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot</p>	N/A	H-DEL-INSP-050320/632

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Function			Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>inspiron_5580</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-INSP-050320/633
Missing Authentication for Critical	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot	N/A	H-DEL-INSP-050320/634

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Function			Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>inspiron_5582</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-INSP-050320/635
Missing Authentication for Critical	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot	N/A	H-DEL-INSP-050320/636

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Function			Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>inspiron_5770</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-INSP-050320/637
<b>inspiron_7380</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility	N/A	H-DEL-INSP-050320/638

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	H-DEL-INSP-050320/639
<b>inspiron_7386</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility</p>	N/A	H-DEL-INSP-050320/640

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>		
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-INSP-050320/641
<b>inspiron_7472</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage	N/A	H-DEL-INSP-050320/642

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>inspiron_7580</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-INSP-050320/643
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage	N/A	H-DEL-INSP-050320/644

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>inspiron_7586</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-INSP-050320/645
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage	N/A	H-DEL-INSP-050320/646

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>inspiron_7786</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-INSP-050320/647
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage	N/A	H-DEL-INSP-050320/648

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>optiplex_7450</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-OPTI-050320/649
<b>optiplex_7040</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST)	N/A	H-DEL-OPTI-050320/650

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>optiplex_5050</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-OPTI-050320/651
<b>vostro_3470</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker	N/A	H-DEL-VOST-050320/652

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>vostro_3480</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-VOST-050320/653
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker	N/A	H-DEL-VOST-050320/654

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>vostro_3580</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-VOST-050320/655
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker	N/A	H-DEL-VOST-050320/656

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>vostro_3581</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-VOST-050320/657
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker	N/A	H-DEL-VOST-050320/658

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>vostro_3584</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-VOST-050320/659
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker	N/A	H-DEL-VOST-050320/660

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>vostro_3583</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	H-DEL-VOST-050320/661
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker	N/A	H-DEL-VOST-050320/662

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>vostro_3670</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-VOST-050320/663
<b>vostro_5370</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the	N/A	H-DEL-VOST-050320/664

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>vostro_5471</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-VOST-050320/665
<b>vostro_5481</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally	N/A	H-DEL-VOST-050320/666

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>		
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-VOST-050320/667
<b>vostro_5581</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally	N/A	H-DEL-VOST-050320/668

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>		
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-VOST-050320/669
<b>wyse_5070</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform	N/A	H-DEL-WYSE-050320/670

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>wyse_7040</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	H-DEL-WYSE-050320/671
<b>Dlink</b>					
<b>dap-1330</b>					
Improper Authentication	22-02-2020	8.3	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DAP-1330 1.10B01 BETA Wi-Fi range extenders. Authentication is not required to exploit this vulnerability. The specific flaw exists within the	N/A	H-DLI-DAP--050320/672

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			handling of HNAP login requests. The issue results from the lack of proper handling of cookies. An attacker can leverage this vulnerability to execute arbitrary code on the router. Was ZDI-CAN-9554. <b>CVE ID : CVE-2020-8861</b>		
<b>dap-2610</b>					
Improper Authentication	22-02-2020	8.3	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DAP-2610 Firmware v2.01RC067 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of passwords. The issue results from the lack of proper password checking. An attacker can leverage this vulnerability to execute arbitrary code in the context of root. Was ZDI-CAN-10082. <b>CVE ID : CVE-2020-8862</b>	N/A	H-DLI-DAP--050320/673
<b>D-link</b>					
<b>dch-m225</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-02-2020	10	D-Link DCH-M225 1.05b01 and earlier devices allow remote attackers to execute arbitrary OS commands via shell metacharacters in the spotifyConnect.php userName parameter. <b>CVE ID : CVE-2020-6841</b>	<a href="https://support.announcements.us.dlink.com/announcement/publication.aspx?name=SAP10152">https://support.announcements.us.dlink.com/announcement/publication.aspx?name=SAP10152</a>	H-D-L-DCH--050320/674

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-02-2020	9	D-Link DCH-M225 1.05b01 and earlier devices allow remote authenticated admins to execute arbitrary OS commands via shell metacharacters in the media renderer name. <b>CVE ID : CVE-2020-6842</b>	<a href="https://support.announcements.us.dlink.com/announcements/publication.aspx?name=SAP10152">https://support.announcements.us.dlink.com/announcements/publication.aspx?name=SAP10152</a>	H-D-L-DCH--050320/675
<b>eltex-co</b>					
<b>ntp-2</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-02-2020	10	ELTEX NTP-RG-1402G 1v10 3.25.3.32 devices allow OS command injection via the PING field of the resource ping.cmd. The NTP-2 device is also affected. <b>CVE ID : CVE-2020-9026</b>	N/A	H-ELT-NTP--050320/676
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-02-2020	10	ELTEX NTP-RG-1402G 1v10 3.25.3.32 devices allow OS command injection via the TRACE field of the resource ping.cmd. The NTP-2 device is also affected. <b>CVE ID : CVE-2020-9027</b>	N/A	H-ELT-NTP--050320/677
<b>ntp-rg-1402g</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-02-2020	10	ELTEX NTP-RG-1402G 1v10 3.25.3.32 devices allow OS command injection via the PING field of the resource ping.cmd. The NTP-2 device is also affected. <b>CVE ID : CVE-2020-9026</b>	N/A	H-ELT-NTP--050320/678

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-02-2020	10	ELTEX NTP-RG-1402G 1v10 3.25.3.32 devices allow OS command injection via the TRACE field of the resource ping.cmd. The NTP-2 device is also affected. <b>CVE ID : CVE-2020-9027</b>	N/A	H-ELT-NTP--050320/679
<b>hitrontech</b>					
<b>coda-4582u</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-02-2020	3.5	Hitron CODA-4582U 7.1.1.30 devices allow XSS via a Managed Device name on the Wireless > Access Control > Add Managed Device screen. <b>CVE ID : CVE-2020-8824</b>	N/A	H-HIT-CODA-050320/680
<b>Honeywell</b>					
<b>inncom_inncontrol</b>					
Improper Privilege Management	20-02-2020	4.6	Honeywell INNCOM INNControl 3 allows workstation users to escalate application user privileges through the modification of local configuration files. <b>CVE ID : CVE-2020-6968</b>	N/A	H-HON-INNC-050320/681
<b>Huawei</b>					
<b>honor_magic2</b>					
Incorrect Authorization	18-02-2020	2.1	Huawei mobile phones Ever-L29B versions earlier than 10.0.0.180(C185E6R3P3), earlier than 10.0.0.180(C432E6R1P7), earlier than 10.0.0.180(C636E5R2P3);	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-</a>	H-HUA-HONO-050320/682

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HUAWEI Mate 20 RS versions earlier than 10.0.0.175(C786E70R3P8); HUAWEI Mate 20 X versions earlier than 10.0.0.176(C00E70R2P8); and Honor Magic2 versions earlier than 10.0.0.175(C00E59R2P11) have an improper authorization vulnerability. Due to improper authorization of some function, attackers can bypass the authorization to perform some operations. <b>CVE ID : CVE-2020-1882</b>	01-phone-en	
<b>nip6300</b>					
Information Exposure	17-02-2020	5	Huawei NGFW Module, NIP6300, NIP6600, Secospace USG6500, Secospace USG6600, and USG9500 versions V500R001C30, V500R001C60, and V500R005C00 have an information leakage vulnerability. An attacker can exploit this vulnerability by sending specific request packets to affected devices. Successful exploit may lead to information leakage. <b>CVE ID : CVE-2020-1856</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-firewall-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-firewall-en</a>	H-HUA-NIP6-050320/683
<b>nip6600</b>					
Information Exposure	17-02-2020	5	Huawei NGFW Module, NIP6300, NIP6600, Secospace USG6500, Secospace USG6600, and	<a href="http://www.huawei.com/en/psirt/security-">http://www.huawei.com/en/psirt/security-</a>	H-HUA-NIP6-050320/684

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			USG9500 versions V500R001C30, V500R001C60, and V500R005C00 have an information leakage vulnerability. An attacker can exploit this vulnerability by sending specific request packets to affected devices. Successful exploit may lead to information leakage. <b>CVE ID : CVE-2020-1856</b>	advisories/huawei-sa-20200205-01-firewall-en	
<b>nip6800</b>					
NULL Pointer Dereference	18-02-2020	3.5	Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00; Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00 have a Dangling pointer dereference vulnerability. An authenticated attacker may do some special operations in the affected products in some special scenarios to exploit the vulnerability. Due to improper race conditions of different operations, successful exploit will lead to Dangling pointer dereference, causing some service abnormal. <b>CVE ID : CVE-2020-1814</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-01-firewall-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-01-firewall-en</a>	H-HUA-NIP6-050320/685
Missing Release of	18-02-2020	4.3	Huawei NIP6800 versions V500R001C30,	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-01-firewall-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-01-firewall-en</a>	H-HUA-NIP6-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource after Effective Lifetime			<p>V500R001C60SPC500, and V500R005C00; Secospace USG6600 and USG9500 versions</p> <p>V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00 have a memory leak vulnerability. The software does not sufficiently track and release allocated memory while parse certain message, the attacker sends the message continuously that could consume remaining memory. Successful exploit could cause memory exhaust.</p> <p><b>CVE ID : CVE-2020-1815</b></p>	om/en/psirt/security-advisories/huawei-sa-20200212-02-firewall-en	050320/686
Improper Input Validation	18-02-2020	4.3	<p>Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00; Secospace USG6600 and USG9500 versions</p> <p>V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00 have a Denial of Service (DoS) vulnerability. Due to improper processing of specific IPSEC packets, remote attackers can send constructed IPSEC packets to affected devices to exploit this vulnerability. Successful exploit could cause the IPsec function of the affected</p>	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-03-firewall-en	H-HUA-NIP6-050320/687

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device abnormal. <b>CVE ID : CVE-2020-1816</b>		
Improper Resource Shutdown or Release	17-02-2020	5	Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00SPC100; and Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00SPC100 have an information leakage vulnerability. An attacker can exploit this vulnerability by sending specific request packets to affected devices. Successful exploit may lead to information leakage. <b>CVE ID : CVE-2020-1827</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-02-ipsec-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-02-ipsec-en</a>	H-HUA-NIP6-050320/688
Improper Input Validation	17-02-2020	5	Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00; and Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00 have an input validation vulnerability where the IPSec module does not validate a field in a specific message. Attackers can send specific message to cause out-of-bound read, compromising normal service. <b>CVE ID : CVE-2020-1828</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-01-ipsec-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-01-ipsec-en</a>	H-HUA-NIP6-050320/689

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	17-02-2020	5	Huawei NIP6800 versions V500R001C30 and V500R001C60SPC500; and Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, and V500R001C60SPC500 have a vulnerability that the IPSec module handles a message improperly. Attackers can send specific message to cause double free memory. This may compromise normal service. <b>CVE ID : CVE-2020-1829</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-03-ipsec-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-03-ipsec-en</a>	H-HUA-NIP6-050320/690
Out-of-bounds Read	18-02-2020	5	Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00; Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00 have a vulnerability that a memory management error exists when IPSec Module handing a specific message. This causes 1 byte out-of-bound read, compromising normal service. <b>CVE ID : CVE-2020-1830</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-04-ipsec-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-04-ipsec-en</a>	H-HUA-NIP6-050320/691
Information Exposure	17-02-2020	2.1	Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00SPC100; and Secospace USG6600 and USG9500 versions	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-</a>	H-HUA-NIP6-050320/692

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00SPC100 have an information leakage vulnerability. Due to improper processing of some data, a local authenticated attacker can exploit this vulnerability through a series of operations. Successful exploitation may cause information leakage. <b>CVE ID : CVE-2020-1857</b>	20200205-01-leakage-en	
N/A	17-02-2020	5	Huawei products NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00SPC100; Secospace USG6600 versions V500R001C30SPC600, V500R001C60SPC500, and V500R005C00SPC100; and USG9500 versions V500R001C30SPC600, V500R001C60SPC500, and V500R005C00SPC100 have a denial of service vulnerability. Attackers need to perform a series of operations in a special scenario to exploit this vulnerability. Successful exploit may cause the new connections can't be established, result in a denial of service. <b>CVE ID : CVE-2020-1858</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-dos-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-dos-en</a> , <a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200219-04-dos-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200219-04-dos-en</a>	H-HUA-NIP6-050320/693
Access of Uninitialized	28-02-2020	4.9	NIP6800;Secospace USG6600;USG9500 products	N/A	H-HUA-NIP6-050320/694

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pointer			versions of V500R001C30; V500R001C60SPC500; V500R005C00SPC100 have a invalid pointer access vulnerability. The software system access an invalid pointer when operator logs in to the device and performs some operations. Successful exploit could cause certain process reboot. <b>CVE ID : CVE-2020-1874</b>		
Access of Uninitialized Pointer	28-02-2020	4.9	NIP6800;Secospace USG6600;USG9500 with versions of V500R001C30; V500R001C60SPC500; V500R005C00SPC100 have an invalid pointer access vulnerability. The software system access an invalid pointer when administrator log in to the device and performs some operations. Successful exploit could cause certain process reboot. <b>CVE ID : CVE-2020-1877</b>	N/A	H-HUA-NIP6- 050320/695
Uncontrolled Resource Consumption	28-02-2020	5	NIP6800;Secospace USG6600;USG9500 products with versions of V500R001C30; V500R001C60SPC500; V500R005C00SPC100 have have a resource management error vulnerability. An attacker needs to perform specific operations to trigger a function of the affected device. Due to improper resource management of the	N/A	H-HUA-NIP6- 050320/696

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			function, the vulnerability can be exploited to cause service abnormal on affected devices. <b>CVE ID : CVE-2020-1881</b>		
<b>secospace_usg6500</b>					
Information Exposure	17-02-2020	5	Huawei NGFW Module, NIP6300, NIP6600, Secospace USG6500, Secospace USG6600, and USG9500 versions V500R001C30, V500R001C60, and V500R005C00 have an information leakage vulnerability. An attacker can exploit this vulnerability by sending specific request packets to affected devices. Successful exploit may lead to information leakage. <b>CVE ID : CVE-2020-1856</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-firewall-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-firewall-en</a>	H-HUA-SECO-050320/697
<b>secospace_usg6600</b>					
NULL Pointer Dereference	18-02-2020	3.5	Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00; Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00 have a Dangling pointer dereference vulnerability. An authenticated attacker may do some special operations in the affected products in some special	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-01-firewall-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-01-firewall-en</a>	H-HUA-SECO-050320/698

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			scenarios to exploit the vulnerability. Due to improper race conditions of different operations, successful exploit will lead to Dangling pointer dereference, causing some service abnormal. <b>CVE ID : CVE-2020-1814</b>		
Missing Release of Resource after Effective Lifetime	18-02-2020	4.3	Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00; Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00 have a memory leak vulnerability. The software does not sufficiently track and release allocated memory while parse certain message, the attacker sends the message continuously that could consume remaining memory. Successful exploit could cause memory exhaust. <b>CVE ID : CVE-2020-1815</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-02-firewall-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-02-firewall-en</a>	H-HUA-SECO-050320/699
Improper Input Validation	18-02-2020	4.3	Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00; Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-03-firewall-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-03-firewall-en</a>	H-HUA-SECO-050320/700

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R005C00 have a Denial of Service (DoS) vulnerability. Due to improper processing of specific IPSEC packets, remote attackers can send constructed IPSEC packets to affected devices to exploit this vulnerability. Successful exploit could cause the IPsec function of the affected device abnormal. <b>CVE ID : CVE-2020-1816</b>		
Improper Resource Shutdown or Release	17-02-2020	5	Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00SPC100; and Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00SPC100 have an information leakage vulnerability. An attacker can exploit this vulnerability by sending specific request packets to affected devices. Successful exploit may lead to information leakage. <b>CVE ID : CVE-2020-1827</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-02-ipsec-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-02-ipsec-en</a>	H-HUA-SECO-050320/701
Improper Input Validation	17-02-2020	5	Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00; and Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-01-ipsec-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-01-ipsec-en</a>	H-HUA-SECO-050320/702

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R005C00 have an input validation vulnerability where the IPSec module does not validate a field in a specific message. Attackers can send specific message to cause out-of-bound read, compromising normal service. <b>CVE ID : CVE-2020-1828</b>		
Double Free	17-02-2020	5	Huawei NIP6800 versions V500R001C30 and V500R001C60SPC500; and Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, and V500R001C60SPC500 have a vulnerability that the IPSec module handles a message improperly. Attackers can send specific message to cause double free memory. This may compromise normal service. <b>CVE ID : CVE-2020-1829</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-03-ipsec-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-03-ipsec-en</a>	H-HUA-SECO-050320/703
Out-of-bounds Read	18-02-2020	5	Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00; Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00 have a vulnerability that a memory management error exists when IPSec Module handing a specific message. This	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-04-ipsec-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-04-ipsec-en</a>	H-HUA-SECO-050320/704

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			causes 1 byte out-of-bound read, compromising normal service. <b>CVE ID : CVE-2020-1830</b>		
Information Exposure	17-02-2020	5	Huawei NGFW Module, NIP6300, NIP6600, Secospace USG6500, Secospace USG6600, and USG9500 versions V500R001C30, V500R001C60, and V500R005C00 have an information leakage vulnerability. An attacker can exploit this vulnerability by sending specific request packets to affected devices. Successful exploit may lead to information leakage. <b>CVE ID : CVE-2020-1856</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-firewall-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-firewall-en</a>	H-HUA-SECO-050320/705
Information Exposure	17-02-2020	2.1	Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00SPC100; and Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00SPC100 have an information leakage vulnerability. Due to improper processing of some data, a local authenticated attacker can exploit this vulnerability through a series of operations. Successful exploitation may cause information leakage.	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-leakage-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-leakage-en</a>	H-HUA-SECO-050320/706

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-1857</b>		
N/A	17-02-2020	5	<p>Huawei products NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00SPC100; Secospace USG6600 versions V500R001C30SPC600, V500R001C60SPC500, and V500R005C00SPC100; and USG9500 versions V500R001C30SPC600, V500R001C60SPC500, and V500R005C00SPC100 have a denial of service vulnerability. Attackers need to perform a series of operations in a special scenario to exploit this vulnerability. Successful exploit may cause the new connections can't be established, result in a denial of service.</p> <p><b>CVE ID : CVE-2020-1858</b></p>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-dos-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-dos-en</a> , <a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200219-04-dos-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200219-04-dos-en</a>	H-HUA-SECO-050320/707
Access of Uninitialized Pointer	28-02-2020	4.9	<p>NIP6800;Secospace USG6600;USG9500 products versions of V500R001C30; V500R001C60SPC500; V500R005C00SPC100 have a invalid pointer access vulnerability. The software system access an invalid pointer when operator logs in to the device and performs some operations. Successful exploit could cause certain process reboot.</p> <p><b>CVE ID : CVE-2020-1874</b></p>	N/A	H-HUA-SECO-050320/708
Access of Uninitialized	28-02-2020	4.9	NIP6800;Secospace USG6600;USG9500 with	N/A	H-HUA-SECO-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pointer			versions of V500R001C30; V500R001C60SPC500; V500R005C00SPC100 have an invalid pointer access vulnerability. The software system access an invalid pointer when administrator log in to the device and performs some operations. Successful exploit could cause certain process reboot. <b>CVE ID : CVE-2020-1877</b>		050320/709
Uncontrolled Resource Consumption	28-02-2020	5	NIP6800;Secospace USG6600;USG9500 products with versions of V500R001C30; V500R001C60SPC500; V500R005C00SPC100 have have a resource management error vulnerability. An attacker needs to perform specific operations to trigger a function of the affected device. Due to improper resource management of the function, the vulnerability can be exploited to cause service abnormal on affected devices. <b>CVE ID : CVE-2020-1881</b>	N/A	H-HUA-SECO-050320/710
<b>p30</b>					
Improper Authentication	18-02-2020	6.8	HUAWEI P30 smartphones with versions earlier than 10.0.0.173(C00E73R1P11) have an improper authentication vulnerability. Due to improperly validation of certain application, an attacker should trick the	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200120-01-">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200120-01-</a>	H-HUA-P30-050320/711

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user into installing a malicious application to exploit this vulnerability. Successful exploit could allow the attacker to bypass the authentication to perform unauthorized operations. <b>CVE ID : CVE-2020-1812</b>	smartphone -en	
<b>mate_20_x</b>					
Incorrect Authorization	18-02-2020	2.1	Huawei mobile phones Ever-L29B versions earlier than 10.0.0.180(C185E6R3P3), earlier than 10.0.0.180(C432E6R1P7), earlier than 10.0.0.180(C636E5R2P3); HUAWEI Mate 20 RS versions earlier than 10.0.0.175(C786E70R3P8); HUAWEI Mate 20 X versions earlier than 10.0.0.176(C00E70R2P8); and Honor Magic2 versions earlier than 10.0.0.175(C00E59R2P11) have an improper authorization vulnerability. Due to improper authorization of some function, attackers can bypass the authorization to perform some operations. <b>CVE ID : CVE-2020-1882</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-phone-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-phone-en</a>	H-HUA-MATE-050320/712
<b>mate_20</b>					
Incorrect Authorization	18-02-2020	2.1	HUAWEI Mate 20 smartphones with versions earlier than 10.0.0.185(C00E74R3P8)	<a href="http://www.huawei.com/en/psirt/security-">http://www.huawei.com/en/psirt/security-</a>	H-HUA-MATE-050320/713

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have an improper authorization vulnerability. The system has a logic judging error under certain scenario, successful exploit could allow the attacker to switch to third desktop after a series of operation in ADB mode. <b>CVE ID : CVE-2020-1791</b>	advisories/huawei-sa-20200205-01-smartphone-en	
<b>osca-550</b>					
Improper Authentication	18-02-2020	4.6	Huawei OSCA-550, OSCA-550A, OSCA-550AX, and OSCA-550X products with version 1.0.1.21(SP3) have an insufficient authentication vulnerability. The software does not require a strong credential when the user trying to do certain operations. Successful exploit could allow an attacker to pass the authentication and do certain operations by a weak credential. <b>CVE ID : CVE-2020-1789</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200121-01-osca-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200121-01-osca-en</a>	H-HUA-OSCA-050320/714
Improper Authentication	18-02-2020	4.6	Huawei HEGE-560 version 1.0.1.20(SP2); OSCA-550 and OSCA-550A version 1.0.0.71(SP1); and OSCA-550AX and OSCA-550X version 1.0.0.71(SP2) have an insufficient authentication vulnerability. An attacker can access the device physically and perform specific operations to exploit this vulnerability. Successful exploitation may	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-osca-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-osca-en</a>	H-HUA-OSCA-050320/715

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cause the attacker obtain high privilege. <b>CVE ID : CVE-2020-1842</b>		
Improper Input Validation	18-02-2020	4.6	Huawei HEGE-560 version 1.0.1.20(SP2), OSCA-550 version 1.0.0.71(SP1), OSCA-550A version 1.0.0.71(SP1), OSCA-550AX version 1.0.0.71(SP2), and OSCA-550X version 1.0.0.71(SP2) have an insufficient verification vulnerability. An attacker can perform specific operations to exploit this vulnerability by physical access methods. Successful exploitation may cause the attacker perform an illegal operation. <b>CVE ID : CVE-2020-1843</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-02-osca-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-02-osca-en</a>	H-HUA-OSCA-050320/716
Improper Input Validation	18-02-2020	3.6	Huawei HEGE-570 version 1.0.1.22(SP3); and HEGE-560, OSCA-550, OSCA-550A, OSCA-550AX, and OSCA-550X version 1.0.1.21(SP3) have an insufficient verification vulnerability. An attacker can access the device physically and exploit this vulnerability to tamper with device information. Successful exploit may cause service abnormal. <b>CVE ID : CVE-2020-1855</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-03-osca-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-03-osca-en</a>	H-HUA-OSCA-050320/717
<b>osca-550a</b>					
Improper Authentication	18-02-2020	4.6	Huawei OSCA-550, OSCA-550A, OSCA-550AX, and OSCA-550X products with version 1.0.1.21(SP3) have	<a href="http://www.huawei.com/en/psirt/security-">http://www.huawei.com/en/psirt/security-</a>	H-HUA-OSCA-050320/718

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an insufficient authentication vulnerability. The software does not require a strong credential when the user trying to do certain operations. Successful exploit could allow an attacker to pass the authentication and do certain operations by a weak credential. <b>CVE ID : CVE-2020-1789</b>	advisories/huawei-sa-20200121-01-osca-en	
Improper Authentication	18-02-2020	4.6	Huawei HEGE-560 version 1.0.1.20(SP2); OSCA-550 and OSCA-550A version 1.0.0.71(SP1); and OSCA-550AX and OSCA-550X version 1.0.0.71(SP2) have an insufficient authentication vulnerability. An attacker can access the device physically and perform specific operations to exploit this vulnerability. Successful exploitation may cause the attacker obtain high privilege. <b>CVE ID : CVE-2020-1842</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-osca-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-osca-en</a>	H-HUA-OSCA-050320/719
Improper Input Validation	18-02-2020	4.6	Huawei HEGE-560 version 1.0.1.20(SP2), OSCA-550 version 1.0.0.71(SP1), OSCA-550A version 1.0.0.71(SP1), OSCA-550AX version 1.0.0.71(SP2), and OSCA-550X version 1.0.0.71(SP2) have an insufficient verification vulnerability. An attacker can perform specific operations to exploit this vulnerability by physical	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-02-osca-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-02-osca-en</a>	H-HUA-OSCA-050320/720

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access methods. Successful exploitation may cause the attacker perform an illegal operation. <b>CVE ID : CVE-2020-1843</b>		
Improper Input Validation	18-02-2020	3.6	Huawei HEGE-570 version 1.0.1.22(SP3); and HEGE-560, OSCA-550, OSCA-550A, OSCA-550AX, and OSCA-550X version 1.0.1.21(SP3) have an insufficient verification vulnerability. An attacker can access the device physically and exploit this vulnerability to tamper with device information. Successful exploit may cause service abnormal. <b>CVE ID : CVE-2020-1855</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-03-osca-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-03-osca-en</a>	H-HUA-OSCA-050320/721
<b>osca-550ax</b>					
Improper Authentication	18-02-2020	4.6	Huawei OSCA-550, OSCA-550A, OSCA-550AX, and OSCA-550X products with version 1.0.1.21(SP3) have an insufficient authentication vulnerability. The software does not require a strong credential when the user trying to do certain operations. Successful exploit could allow an attacker to pass the authentication and do certain operations by a weak credential. <b>CVE ID : CVE-2020-1789</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200121-01-osca-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200121-01-osca-en</a>	H-HUA-OSCA-050320/722
Improper Authentication	18-02-2020	4.6	Huawei HEGE-560 version 1.0.1.20(SP2); OSCA-550 and OSCA-550A version	<a href="http://www.huawei.com/en/psirt">http://www.huawei.com/en/psirt</a>	H-HUA-OSCA-050320/723

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.0.71(SP1); and OSCA-550AX and OSCA-550X version 1.0.0.71(SP2) have an insufficient authentication vulnerability. An attacker can access the device physically and perform specific operations to exploit this vulnerability. Successful exploitation may cause the attacker obtain high privilege. <b>CVE ID : CVE-2020-1842</b>	t/security-advisories/huawei-sa-20200122-01-osca-en	
Improper Input Validation	18-02-2020	4.6	Huawei HEGE-560 version 1.0.1.20(SP2), OSCA-550 version 1.0.0.71(SP1), OSCA-550A version 1.0.0.71(SP1), OSCA-550AX version 1.0.0.71(SP2), and OSCA-550X version 1.0.0.71(SP2) have an insufficient verification vulnerability. An attacker can perform specific operations to exploit this vulnerability by physical access methods. Successful exploitation may cause the attacker perform an illegal operation. <b>CVE ID : CVE-2020-1843</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-02-osca-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-02-osca-en</a>	H-HUA-OSCA-050320/724
Improper Input Validation	18-02-2020	3.6	Huawei HEGE-570 version 1.0.1.22(SP3); and HEGE-560, OSCA-550, OSCA-550A, OSCA-550AX, and OSCA-550X version 1.0.1.21(SP3) have an insufficient verification vulnerability. An attacker can access the device physically and exploit this vulnerability to tamper	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-03-osca-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-03-osca-en</a>	H-HUA-OSCA-050320/725

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with device information. Successful exploit may cause service abnormal. <b>CVE ID : CVE-2020-1855</b>		
<b>osca-550x</b>					
Improper Authentication	18-02-2020	4.6	Huawei OSCA-550, OSCA-550A, OSCA-550AX, and OSCA-550X products with version 1.0.1.21(SP3) have an insufficient authentication vulnerability. The software does not require a strong credential when the user trying to do certain operations. Successful exploit could allow an attacker to pass the authentication and do certain operations by a weak credential. <b>CVE ID : CVE-2020-1789</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200121-01-osca-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200121-01-osca-en</a>	H-HUA-OSCA-050320/726
Improper Authentication	18-02-2020	4.6	Huawei HEGE-560 version 1.0.1.20(SP2); OSCA-550 and OSCA-550A version 1.0.0.71(SP1); and OSCA-550AX and OSCA-550X version 1.0.0.71(SP2) have an insufficient authentication vulnerability. An attacker can access the device physically and perform specific operations to exploit this vulnerability. Successful exploitation may cause the attacker obtain high privilege. <b>CVE ID : CVE-2020-1842</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-osca-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-osca-en</a>	H-HUA-OSCA-050320/727
Improper Input	18-02-2020	4.6	Huawei HEGE-560 version 1.0.1.20(SP2), OSCA-550	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-osca-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-osca-en</a>	H-HUA-OSCA-050320/728

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			version 1.0.0.71(SP1), OSCA-550A version 1.0.0.71(SP1), OSCA-550AX version 1.0.0.71(SP2), and OSCA-550X version 1.0.0.71(SP2) have an insufficient verification vulnerability. An attacker can perform specific operations to exploit this vulnerability by physical access methods. Successful exploitation may cause the attacker perform an illegal operation. <b>CVE ID : CVE-2020-1843</b>	om/en/psirt/security-advisories/huawei-sa-20200122-02-osca-en	
Improper Input Validation	18-02-2020	3.6	Huawei HEGE-570 version 1.0.1.22(SP3); and HEGE-560, OSCA-550, OSCA-550A, OSCA-550AX, and OSCA-550X version 1.0.1.21(SP3) have an insufficient verification vulnerability. An attacker can access the device physically and exploit this vulnerability to tamper with device information. Successful exploit may cause service abnormal. <b>CVE ID : CVE-2020-1855</b>	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-03-osca-en	H-HUA-OSCA-050320/729
<b>cloudlink_board</b>					
Information Exposure	17-02-2020	5	Huawei CloudLink Board version 20.0.0; DP300 version V500R002C00; RSE6500 versions V100R001C00, V500R002C00, and V500R002C00SPC900; and TE60 versions V500R002C00, V600R006C00,	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200207-01-te-en	H-HUA-CLOU-050320/730

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V600R006C00SPC200, V600R006C00SPC300, V600R006C10, V600R019C00, and V600R019C00SPC100 have an information leak vulnerability. An unauthenticated, remote attacker can make a large number of attempts to guess information. Successful exploitation may cause information leak. <b>CVE ID : CVE-2020-1841</b>		
<b>dp300</b>					
Information Exposure	17-02-2020	5	Huawei CloudLink Board version 20.0.0; DP300 version V500R002C00; RSE6500 versions V100R001C00, V500R002C00, and V500R002C00SPC900; and TE60 versions V500R002C00, V600R006C00, V600R006C00SPC200, V600R006C00SPC300, V600R006C10, V600R019C00, and V600R019C00SPC100 have an information leak vulnerability. An unauthenticated, remote attacker can make a large number of attempts to guess information. Successful exploitation may cause information leak. <b>CVE ID : CVE-2020-1841</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200207-01-te-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200207-01-te-en</a>	H-HUA-DP30-050320/731

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<b>rse6500</b>					
Information Exposure	17-02-2020	5	<p>Huawei CloudLink Board version 20.0.0; DP300 version V500R002C00; RSE6500 versions V100R001C00, V500R002C00, and V500R002C00SPC900; and TE60 versions V500R002C00, V600R006C00, V600R006C00SPC200, V600R006C00SPC300, V600R006C10, V600R019C00, and V600R019C00SPC100 have an information leak vulnerability. An unauthenticated, remote attacker can make a large number of attempts to guess information. Successful exploitation may cause information leak.</p> <p><b>CVE ID : CVE-2020-1841</b></p>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200207-01-te-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200207-01-te-en</a>	H-HUA-RSE6-050320/732
<b>te60</b>					
Information Exposure	17-02-2020	5	<p>Huawei CloudLink Board version 20.0.0; DP300 version V500R002C00; RSE6500 versions V100R001C00, V500R002C00, and V500R002C00SPC900; and TE60 versions V500R002C00, V600R006C00, V600R006C00SPC200, V600R006C00SPC300, V600R006C10, V600R019C00, and</p>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200207-01-te-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200207-01-te-en</a>	H-HUA-TE60-050320/733

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V600R019C00SPC100 have an information leak vulnerability. An unauthenticated, remote attacker can make a large number of attempts to guess information. Successful exploitation may cause information leak. <b>CVE ID : CVE-2020-1841</b>		
<b>hege-560</b>					
Improper Authentication	18-02-2020	4.6	Huawei HEGE-560 version 1.0.1.20(SP2); OSCA-550 and OSCA-550A version 1.0.0.71(SP1); and OSCA-550AX and OSCA-550X version 1.0.0.71(SP2) have an insufficient authentication vulnerability. An attacker can access the device physically and perform specific operations to exploit this vulnerability. Successful exploitation may cause the attacker obtain high privilege. <b>CVE ID : CVE-2020-1842</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-osca-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-osca-en</a>	H-HUA-HEGE-050320/734
Improper Input Validation	18-02-2020	4.6	Huawei HEGE-560 version 1.0.1.20(SP2), OSCA-550 version 1.0.0.71(SP1), OSCA-550A version 1.0.0.71(SP1), OSCA-550AX version 1.0.0.71(SP2), and OSCA-550X version 1.0.0.71(SP2) have an insufficient verification vulnerability. An attacker can perform specific operations to exploit this vulnerability by physical access methods. Successful	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-02-osca-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-02-osca-en</a>	H-HUA-HEGE-050320/735

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation may cause the attacker perform an illegal operation. <b>CVE ID : CVE-2020-1843</b>		
Improper Input Validation	18-02-2020	3.6	Huawei HEGE-570 version 1.0.1.22(SP3); and HEGE-560, OSCA-550, OSCA-550A, OSCA-550AX, and OSCA-550X version 1.0.1.21(SP3) have an insufficient verification vulnerability. An attacker can access the device physically and exploit this vulnerability to tamper with device information. Successful exploit may cause service abnormal. <b>CVE ID : CVE-2020-1855</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-03-osca-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-03-osca-en</a>	H-HUA-HEGE-050320/736
<b>hege-570</b>					
Improper Input Validation	18-02-2020	3.6	Huawei HEGE-570 version 1.0.1.22(SP3); and HEGE-560, OSCA-550, OSCA-550A, OSCA-550AX, and OSCA-550X version 1.0.1.21(SP3) have an insufficient verification vulnerability. An attacker can access the device physically and exploit this vulnerability to tamper with device information. Successful exploit may cause service abnormal. <b>CVE ID : CVE-2020-1855</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-03-osca-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-03-osca-en</a>	H-HUA-HEGE-050320/737
<b>ngfw_module</b>					
Information Exposure	17-02-2020	5	Huawei NGFW Module, NIP6300, NIP6600, Secospace USG6500, Secospace USG6600, and USG9500 versions	<a href="http://www.huawei.com/en/psirt/security-advisories/">http://www.huawei.com/en/psirt/security-advisories/</a>	H-HUA-NGFW-050320/738

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R001C30, V500R001C60, and V500R005C00 have an information leakage vulnerability. An attacker can exploit this vulnerability by sending specific request packets to affected devices. Successful exploit may lead to information leakage. <b>CVE ID : CVE-2020-1856</b>	huawei-sa-20200205-01-firewall-en	
<b>p10_plus</b>					
Improper Input Validation	18-02-2020	2.1	Huawei smart phones P10 Plus with versions earlier than 9.1.0.201(C01E75R1P12T8), earlier than 9.1.0.252(C185E2R1P9T8), earlier than 9.1.0.252(C432E4R1P9T8), and earlier than 9.1.0.255(C576E6R1P8T8) have a digital balance bypass vulnerability. When re-configuring the mobile phone at the digital balance mode, an attacker can perform some operations to bypass the startup wizard, and then open some switch. As a result, the digital balance function is bypassed. <b>CVE ID : CVE-2020-1872</b>	<a href="https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-digitalbalance-en">https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-digitalbalance-en</a>	H-HUA-P10_-050320/739
<b>mate_20_rs</b>					
Incorrect Authorization	18-02-2020	2.1	Huawei mobile phones Ever-L29B versions earlier than 10.0.0.180(C185E6R3P3), earlier than 10.0.0.180(C432E6R1P7),	<a href="http://www.huawei.com/en/psirt/security-advisories/">http://www.huawei.com/en/psirt/security-advisories/</a>	H-HUA-MATE-050320/740

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>earlier than 10.0.0.180(C636E5R2P3); HUAWEI Mate 20 RS versions earlier than 10.0.0.175(C786E70R3P8); HUAWEI Mate 20 X versions earlier than 10.0.0.176(C00E70R2P8); and Honor Magic2 versions earlier than 10.0.0.175(C00E59R2P11) have an improper authorization vulnerability. Due to improper authorization of some function, attackers can bypass the authorization to perform some operations.</p> <p><b>CVE ID : CVE-2020-1882</b></p>	huawei-sa-20200122-01-phone-en	
<b>ever-l29b</b>					
Incorrect Authorization	18-02-2020	2.1	<p>Huawei mobile phones Ever-L29B versions earlier than 10.0.0.180(C185E6R3P3), earlier than 10.0.0.180(C432E6R1P7), earlier than 10.0.0.180(C636E5R2P3); HUAWEI Mate 20 RS versions earlier than 10.0.0.175(C786E70R3P8); HUAWEI Mate 20 X versions earlier than 10.0.0.176(C00E70R2P8); and Honor Magic2 versions earlier than 10.0.0.175(C00E59R2P11) have an improper authorization vulnerability. Due to improper authorization of some</p>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-phone-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-phone-en</a>	H-HUA-EVER-050320/741

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			function, attackers can bypass the authorization to perform some operations. <b>CVE ID : CVE-2020-1882</b>		
<b>usg9500</b>					
NULL Pointer Dereference	18-02-2020	3.5	Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00; Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00 have a Dangling pointer dereference vulnerability. An authenticated attacker may do some special operations in the affected products in some special scenarios to exploit the vulnerability. Due to improper race conditions of different operations, successful exploit will lead to Dangling pointer dereference, causing some service abnormal. <b>CVE ID : CVE-2020-1814</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-01-firewall-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-01-firewall-en</a>	H-HUA-USG9-050320/742
Missing Release of Resource after Effective Lifetime	18-02-2020	4.3	Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00; Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00 have a	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-02-firewall-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-02-firewall-en</a>	H-HUA-USG9-050320/743

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory leak vulnerability. The software does not sufficiently track and release allocated memory while parse certain message, the attacker sends the message continuously that could consume remaining memory. Successful exploit could cause memory exhaust. <b>CVE ID : CVE-2020-1815</b>		
Improper Input Validation	18-02-2020	4.3	Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00; Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00 have a Denial of Service (DoS) vulnerability. Due to improper processing of specific IPSEC packets, remote attackers can send constructed IPSEC packets to affected devices to exploit this vulnerability. Successful exploit could cause the IPSec function of the affected device abnormal. <b>CVE ID : CVE-2020-1816</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-03-firewall-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-03-firewall-en</a>	H-HUA-USG9-050320/744
Improper Resource Shutdown or Release	17-02-2020	5	Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00SPC100; and Secospace USG6600 and USG9500 versions	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-</a>	H-HUA-USG9-050320/745

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00SPC100 have an information leakage vulnerability. An attacker can exploit this vulnerability by sending specific request packets to affected devices. Successful exploit may lead to information leakage. <b>CVE ID : CVE-2020-1827</b>	20200212-02-ipsec-en	
Improper Input Validation	17-02-2020	5	Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00; and Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00 have an input validation vulnerability where the IPSec module does not validate a field in a specific message. Attackers can send specific message to cause out-of-bound read, compromising normal service. <b>CVE ID : CVE-2020-1828</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-01-ipsec-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-01-ipsec-en</a>	H-HUA-USG9-050320/746
Double Free	17-02-2020	5	Huawei NIP6800 versions V500R001C30 and V500R001C60SPC500; and Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, and V500R001C60SPC500 have a vulnerability that the IPSec	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-03-ipsec-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-03-ipsec-en</a>	H-HUA-USG9-050320/747

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			module handles a message improperly. Attackers can send specific message to cause double free memory. This may compromise normal service. <b>CVE ID : CVE-2020-1829</b>		
Out-of-bounds Read	18-02-2020	5	Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00; Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00 have a vulnerability that a memory management error exists when IPSec Module handing a specific message. This causes 1 byte out-of-bound read, compromising normal service. <b>CVE ID : CVE-2020-1830</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-04-ipsec-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-04-ipsec-en</a>	H-HUA-USG9-050320/748
Information Exposure	17-02-2020	5	Huawei NGFW Module, NIP6300, NIP6600, Secospace USG6500, Secospace USG6600, and USG9500 versions V500R001C30, V500R001C60, and V500R005C00 have an information leakage vulnerability. An attacker can exploit this vulnerability by sending specific request packets to affected devices. Successful exploit may lead to information leakage.	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-firewall-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-firewall-en</a>	H-HUA-USG9-050320/749

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-1856</b>		
Information Exposure	17-02-2020	2.1	<p>Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00SPC100; and Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00SPC100 have an information leakage vulnerability. Due to improper processing of some data, a local authenticated attacker can exploit this vulnerability through a series of operations. Successful exploitation may cause information leakage.</p> <p><b>CVE ID : CVE-2020-1857</b></p>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-leakage-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-leakage-en</a>	H-HUA-USG9-050320/750
N/A	17-02-2020	5	<p>Huawei products NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00SPC100; Secospace USG6600 versions V500R001C30SPC600, V500R001C60SPC500, and V500R005C00SPC100; and USG9500 versions V500R001C30SPC600, V500R001C60SPC500, and V500R005C00SPC100 have a denial of service vulnerability. Attackers need to perform a series of operations in a special scenario to exploit this vulnerability. Successful</p>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-dos-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-dos-en</a> , <a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200219-04-dos-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200219-04-dos-en</a>	H-HUA-USG9-050320/751

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit may cause the new connections can't be established, result in a denial of service. <b>CVE ID : CVE-2020-1858</b>		
Access of Uninitialized Pointer	28-02-2020	4.9	NIP6800;Secospace USG6600;USG9500 products versions of V500R001C30; V500R001C60SPC500; V500R005C00SPC100 have a invalid pointer access vulnerability. The software system access an invalid pointer when operator logs in to the device and performs some operations. Successful exploit could cause certain process reboot. <b>CVE ID : CVE-2020-1874</b>	N/A	H-HUA-USG9-050320/752
Access of Uninitialized Pointer	28-02-2020	4.9	NIP6800;Secospace USG6600;USG9500 with versions of V500R001C30; V500R001C60SPC500; V500R005C00SPC100 have an invalid pointer access vulnerability. The software system access an invalid pointer when administrator log in to the device and performs some operations. Successful exploit could cause certain process reboot. <b>CVE ID : CVE-2020-1877</b>	N/A	H-HUA-USG9-050320/753
Uncontrolled Resource Consumption	28-02-2020	5	NIP6800;Secospace USG6600;USG9500 products with versions of V500R001C30; V500R001C60SPC500; V500R005C00SPC100 have	N/A	H-HUA-USG9-050320/754

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>have a resource management error vulnerability. An attacker needs to perform specific operations to trigger a function of the affected device. Due to improper resource management of the function, the vulnerability can be exploited to cause service abnormal on affected devices.</p> <p><b>CVE ID : CVE-2020-1881</b></p>		
<b>iteris</b>					
<b>vantage_velocity</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-02-2020	10	<p>Iteris Vantage Velocity Field Unit 2.3.1, 2.4.2, and 3.0 devices allow the injection of OS commands into cgi-bin/timeconfig.py via shell metacharacters in the NTP Server field.</p> <p><b>CVE ID : CVE-2020-9020</b></p>	N/A	H-ITE-VANT-050320/755
Insufficiently Protected Credentials	17-02-2020	7.5	<p>Iteris Vantage Velocity Field Unit 2.3.1 and 2.4.2 devices have two users that are not documented and are configured with weak passwords (User bluetooth, password bluetooth; User eclipse, password eclipse). Also, bluetooth is the root password.</p> <p><b>CVE ID : CVE-2020-9023</b></p>	N/A	H-ITE-VANT-050320/756
Improper Privilege Management	17-02-2020	10	<p>Iteris Vantage Velocity Field Unit 2.3.1 and 2.4.2 devices have world-writable permissions for the</p>	N/A	H-ITE-VANT-050320/757

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			/root/cleardata.pl (executed as root by crond) and /root/loadperl.sh (executed as root at boot time) scripts. <b>CVE ID : CVE-2020-9024</b>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-02-2020	4.3	Iteris Vantage Velocity Field Unit 2.4.2 devices have multiple stored XSS issues in all parameters of the Start Data Viewer feature of the /cgi-bin/loaddata.py script. <b>CVE ID : CVE-2020-9025</b>	N/A	H-ITE-VANT-050320/758
<b>Microchip</b>					
<b>syncserver_s100</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-02-2020	4.3	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow stored XSS via the newUserName parameter on the "User Creation, Deletion and Password Maintenance" screen (when creating a new user). <b>CVE ID : CVE-2020-9028</b>	N/A	H-MIC-SYNC-050320/759
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to messagelog.php. <b>CVE ID : CVE-2020-9029</b>	N/A	H-MIC-SYNC-050320/760
Improper Limitation of a Pathname to a	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow	N/A	H-MIC-SYNC-050320/761

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			Directory Traversal via the FileName parameter to the syslog.php. <b>CVE ID : CVE-2020-9030</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to daemonlog.php. <b>CVE ID : CVE-2020-9031</b>	N/A	H-MIC-SYNC-050320/762
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to kernlog.php. <b>CVE ID : CVE-2020-9032</b>	N/A	H-MIC-SYNC-050320/763
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to authlog.php. <b>CVE ID : CVE-2020-9033</b>	N/A	H-MIC-SYNC-050320/764
Improper Input Validation	17-02-2020	5	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices mishandle session validation, leading to unauthenticated creation, modification, or elimination of users. <b>CVE ID : CVE-2020-9034</b>	N/A	H-MIC-SYNC-050320/765

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<b>syncserver_s200</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-02-2020	4.3	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow stored XSS via the newUserName parameter on the "User Creation, Deletion and Password Maintenance" screen (when creating a new user). <b>CVE ID : CVE-2020-9028</b>	N/A	H-MIC-SYNC-050320/766
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to messagelog.php. <b>CVE ID : CVE-2020-9029</b>	N/A	H-MIC-SYNC-050320/767
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to the syslog.php. <b>CVE ID : CVE-2020-9030</b>	N/A	H-MIC-SYNC-050320/768
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to daemonlog.php. <b>CVE ID : CVE-2020-9031</b>	N/A	H-MIC-SYNC-050320/769
Improper Limitation of	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30,	N/A	H-MIC-SYNC-050320/770

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Pathname to a Restricted Directory ('Path Traversal')			S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to kernlog.php. <b>CVE ID : CVE-2020-9032</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to authlog.php. <b>CVE ID : CVE-2020-9033</b>	N/A	H-MIC-SYNC-050320/771
Improper Input Validation	17-02-2020	5	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices mishandle session validation, leading to unauthenticated creation, modification, or elimination of users. <b>CVE ID : CVE-2020-9034</b>	N/A	H-MIC-SYNC-050320/772
<b>syncserver_s250</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-02-2020	4.3	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow stored XSS via the newUserName parameter on the "User Creation, Deletion and Password Maintenance" screen (when creating a new user). <b>CVE ID : CVE-2020-9028</b>	N/A	H-MIC-SYNC-050320/773
Improper Limitation of	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30,	N/A	H-MIC-SYNC-050320/774

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Pathname to a Restricted Directory ('Path Traversal')			S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to messagelog.php. <b>CVE ID : CVE-2020-9029</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricom SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to the syslog.php. <b>CVE ID : CVE-2020-9030</b>	N/A	H-MIC-SYNC-050320/775
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricom SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to daemonlog.php. <b>CVE ID : CVE-2020-9031</b>	N/A	H-MIC-SYNC-050320/776
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricom SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to kernlog.php. <b>CVE ID : CVE-2020-9032</b>	N/A	H-MIC-SYNC-050320/777
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricom SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to authlog.php. <b>CVE ID : CVE-2020-9033</b>	N/A	H-MIC-SYNC-050320/778

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-02-2020	5	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices mishandle session validation, leading to unauthenticated creation, modification, or elimination of users. <b>CVE ID : CVE-2020-9034</b>	N/A	H-MIC-SYNC-050320/779
<b>syncserver_s300</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-02-2020	4.3	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow stored XSS via the newUserName parameter on the "User Creation, Deletion and Password Maintenance" screen (when creating a new user). <b>CVE ID : CVE-2020-9028</b>	N/A	H-MIC-SYNC-050320/780
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to messageLog.php. <b>CVE ID : CVE-2020-9029</b>	N/A	H-MIC-SYNC-050320/781
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to the syslog.php. <b>CVE ID : CVE-2020-9030</b>	N/A	H-MIC-SYNC-050320/782

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to daemonlog.php. <b>CVE ID : CVE-2020-9031</b>	N/A	H-MIC-SYNC-050320/783
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to kernlog.php. <b>CVE ID : CVE-2020-9032</b>	N/A	H-MIC-SYNC-050320/784
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to authlog.php. <b>CVE ID : CVE-2020-9033</b>	N/A	H-MIC-SYNC-050320/785
Improper Input Validation	17-02-2020	5	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices mishandle session validation, leading to unauthenticated creation, modification, or elimination of users. <b>CVE ID : CVE-2020-9034</b>	N/A	H-MIC-SYNC-050320/786
<b>syncserver_s350</b>					
Improper Neutralization of Input	17-02-2020	4.3	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and	N/A	H-MIC-SYNC-050320/787

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			S350 2.80.1 devices allow stored XSS via the newUserName parameter on the "User Creation, Deletion and Password Maintenance" screen (when creating a new user). <b>CVE ID : CVE-2020-9028</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to messagelog.php. <b>CVE ID : CVE-2020-9029</b>	N/A	H-MIC-SYNC-050320/788
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to the syslog.php. <b>CVE ID : CVE-2020-9030</b>	N/A	H-MIC-SYNC-050320/789
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to daemonlog.php. <b>CVE ID : CVE-2020-9031</b>	N/A	H-MIC-SYNC-050320/790
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to	N/A	H-MIC-SYNC-050320/791

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			kernlog.php. <b>CVE ID : CVE-2020-9032</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to authlog.php. <b>CVE ID : CVE-2020-9033</b>	N/A	H-MIC-SYNC-050320/792
Improper Input Validation	17-02-2020	5	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices mishandle session validation, leading to unauthenticated creation, modification, or elimination of users. <b>CVE ID : CVE-2020-9034</b>	N/A	H-MIC-SYNC-050320/793
<b>NEC</b>					
<b>aterm_wg2600hs</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-02-2020	8.3	Aterm series (Aterm WF1200C firmware Ver1.2.1 and earlier, Aterm WG1200CR firmware Ver1.2.1 and earlier, Aterm WG2600HS firmware Ver1.3.2 and earlier) allows an attacker on the same network segment to execute arbitrary OS commands with root privileges via UPnP function. <b>CVE ID : CVE-2020-5524</b>	N/A	H-NEC-ATER-050320/794
Improper Neutralization of Special	21-02-2020	7.7	Aterm series (Aterm WF1200C firmware Ver1.2.1 and earlier, Aterm	N/A	H-NEC-ATER-050320/795

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			WG1200CR firmware Ver1.2.1 and earlier, Aterm WG2600HS firmware Ver1.3.2 and earlier) allows an authenticated attacker on the same network segment to execute arbitrary OS commands with root privileges via management screen. <b>CVE ID : CVE-2020-5525</b>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-02-2020	4.3	Cross-site scripting vulnerability in Aterm WG2600HS firmware Ver1.3.2 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. <b>CVE ID : CVE-2020-5533</b>	N/A	H-NEC-ATER-050320/796
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-02-2020	7.7	Aterm WG2600HS firmware Ver1.3.2 and earlier allows an authenticated attacker on the same network segment to execute arbitrary OS commands with root privileges via unspecified vectors. <b>CVE ID : CVE-2020-5534</b>	N/A	H-NEC-ATER-050320/797
<b>aterm_wf1200c</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-02-2020	8.3	Aterm series (Aterm WF1200C firmware Ver1.2.1 and earlier, Aterm WG1200CR firmware Ver1.2.1 and earlier, Aterm WG2600HS firmware Ver1.3.2 and earlier) allows an attacker on the same network segment to execute	N/A	H-NEC-ATER-050320/798

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary OS commands with root privileges via UPnP function. <b>CVE ID : CVE-2020-5524</b>		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-02-2020	7.7	Aterm series (Aterm WF1200C firmware Ver1.2.1 and earlier, Aterm WG1200CR firmware Ver1.2.1 and earlier, Aterm WG2600HS firmware Ver1.3.2 and earlier) allows an authenticated attacker on the same network segment to execute arbitrary OS commands with root privileges via management screen. <b>CVE ID : CVE-2020-5525</b>	N/A	H-NEC-ATER-050320/799
<b>aterm_wg1200cr</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-02-2020	8.3	Aterm series (Aterm WF1200C firmware Ver1.2.1 and earlier, Aterm WG1200CR firmware Ver1.2.1 and earlier, Aterm WG2600HS firmware Ver1.3.2 and earlier) allows an attacker on the same network segment to execute arbitrary OS commands with root privileges via UPnP function. <b>CVE ID : CVE-2020-5524</b>	N/A	H-NEC-ATER-050320/800
Improper Neutralization of Special Elements used in an OS Command ('OS	21-02-2020	7.7	Aterm series (Aterm WF1200C firmware Ver1.2.1 and earlier, Aterm WG1200CR firmware Ver1.2.1 and earlier, Aterm WG2600HS firmware Ver1.3.2 and earlier) allows	N/A	H-NEC-ATER-050320/801

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			an authenticated attacker on the same network segment to execute arbitrary OS commands with root privileges via management screen. <b>CVE ID : CVE-2020-5525</b>		
<b>Phoenixcontact</b>					
<b>ilc_2050_bi</b>					
Incorrect Permission Assignment for Critical Resource	17-02-2020	7.5	An issue was discovered on Phoenix Contact Emalytics Controller ILC 2050 BI before 1.2.3 and BI-L before 1.2.3 devices. There is an insecure mechanism for read and write access to the configuration of the device. The mechanism can be discovered by examining a link on the website of the device. <b>CVE ID : CVE-2020-8768</b>	N/A	H-PHO-ILC_-050320/802
<b>ilc_2050_bi-l</b>					
Incorrect Permission Assignment for Critical Resource	17-02-2020	7.5	An issue was discovered on Phoenix Contact Emalytics Controller ILC 2050 BI before 1.2.3 and BI-L before 1.2.3 devices. There is an insecure mechanism for read and write access to the configuration of the device. The mechanism can be discovered by examining a link on the website of the device. <b>CVE ID : CVE-2020-8768</b>	N/A	H-PHO-ILC_-050320/803
<b>Postoaktraffic</b>					
<b>awam_bluetooth_field_device</b>					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-02-2020	10	Post Oak AWAM Bluetooth Field Device 7400v2.08.21.2018, 7800SD.2015.1.16, 2011.3, 7400v2.02.01.2019, and 7800SD.2012.12.5 is vulnerable to injections of operating system commands through timeconfig.py via shell metacharacters in the htmlNtpServer parameter. <b>CVE ID : CVE-2020-9021</b>	N/A	H-POS-AWAM-050320/804
<b>tonnet</b>					
<b>tat-70432n</b>					
Incorrect Authorization	27-02-2020	10	DVR firmware in TAT-76 and TAT-77 series of products, provided by TONNET, contain misconfigured authentication mechanism. Attackers can crack the default password and gain access to the system. <b>CVE ID : CVE-2020-3923</b>	<a href="https://tvn.twcert.org.tw/taiwanvn/TVN-201910003">https://tvn.twcert.org.tw/taiwanvn/TVN-201910003</a> , <a href="https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2bbcf">https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2bbcf</a>	H-TON-TAT--050320/805
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	27-02-2020	10	DVR firmware in TAT-76 and TAT-77 series of products, provided by TONNET do not properly verify patch files. Attackers can inject a specific command into a patch file and gain access to the system. <b>CVE ID : CVE-2020-3924</b>	<a href="https://tvn.twcert.org.tw/taiwanvn/TVN-201910004">https://tvn.twcert.org.tw/taiwanvn/TVN-201910004</a> , <a href="https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2bbcf">https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2bbcf</a>	H-TON-TAT--050320/806

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				bcf	
<b>tat-71416g1</b>					
Incorrect Authorization	27-02-2020	10	DVR firmware in TAT-76 and TAT-77 series of products, provided by TONNET, contain misconfigured authentication mechanism. Attackers can crack the default password and gain access to the system. <b>CVE ID : CVE-2020-3923</b>	<a href="https://tvn.twcert.org.tw/taiwanvn/TVN-201910003">https://tvn.twcert.org.tw/taiwanvn/TVN-201910003</a> , <a href="https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2b">https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2b</a> bcf	H-TON-TAT--050320/807
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	27-02-2020	10	DVR firmware in TAT-76 and TAT-77 series of products, provided by TONNET do not properly verify patch files. Attackers can inject a specific command into a patch file and gain access to the system. <b>CVE ID : CVE-2020-3924</b>	<a href="https://tvn.twcert.org.tw/taiwanvn/TVN-201910004">https://tvn.twcert.org.tw/taiwanvn/TVN-201910004</a> , <a href="https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2b">https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2b</a> bcf	H-TON-TAT--050320/808
<b>tat-71832g1</b>					
Incorrect Authorization	27-02-2020	10	DVR firmware in TAT-76 and TAT-77 series of products, provided by TONNET, contain misconfigured authentication mechanism. Attackers can crack the default password and gain access to the system. <b>CVE ID : CVE-2020-3923</b>	<a href="https://tvn.twcert.org.tw/taiwanvn/TVN-201910003">https://tvn.twcert.org.tw/taiwanvn/TVN-201910003</a> , <a href="https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2b">https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-</a>	H-TON-TAT--050320/809

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ec7213e2b bcf	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	27-02-2020	10	DVR firmware in TAT-76 and TAT-77 series of products, provided by TONNET do not properly verify patch files. Attackers can inject a specific command into a patch file and gain access to the system. <b>CVE ID : CVE-2020-3924</b>	<a href="https://tvn.twcert.org.tw/taiwanvn/TVN-201910004">https://tvn.twcert.org.tw/taiwanvn/TVN-201910004</a> , <a href="https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2b-bcf">https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2b-bcf</a>	H-TON-TAT--050320/810
<b>tat-76104g3</b>					
Incorrect Authorization	27-02-2020	10	DVR firmware in TAT-76 and TAT-77 series of products, provided by TONNET, contain misconfigured authentication mechanism. Attackers can crack the default password and gain access to the system. <b>CVE ID : CVE-2020-3923</b>	<a href="https://tvn.twcert.org.tw/taiwanvn/TVN-201910003">https://tvn.twcert.org.tw/taiwanvn/TVN-201910003</a> , <a href="https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2b-bcf">https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2b-bcf</a>	H-TON-TAT--050320/811
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	27-02-2020	10	DVR firmware in TAT-76 and TAT-77 series of products, provided by TONNET do not properly verify patch files. Attackers can inject a specific command into a patch file and gain access to the system. <b>CVE ID : CVE-2020-3924</b>	<a href="https://tvn.twcert.org.tw/taiwanvn/TVN-201910004">https://tvn.twcert.org.tw/taiwanvn/TVN-201910004</a> , <a href="https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2b-bcf">https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2b-bcf</a>	H-TON-TAT--050320/812

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ec7213e2b bcf	
<b>tat-76108g3</b>					
Incorrect Authorization	27-02-2020	10	DVR firmware in TAT-76 and TAT-77 series of products, provided by TONNET, contain misconfigured authentication mechanism. Attackers can crack the default password and gain access to the system. <b>CVE ID : CVE-2020-3923</b>	<a href="https://tvn.twcert.org.tw/taiwanvn/TVN-201910003">https://tvn.twcert.org.tw/taiwanvn/TVN-201910003</a> , <a href="https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2b-bcf">https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2b-bcf</a>	H-TON-TAT--050320/813
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	27-02-2020	10	DVR firmware in TAT-76 and TAT-77 series of products, provided by TONNET do not properly verify patch files. Attackers can inject a specific command into a patch file and gain access to the system. <b>CVE ID : CVE-2020-3924</b>	<a href="https://tvn.twcert.org.tw/taiwanvn/TVN-201910004">https://tvn.twcert.org.tw/taiwanvn/TVN-201910004</a> , <a href="https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2b-bcf">https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2b-bcf</a>	H-TON-TAT--050320/814
<b>tat-76116g3</b>					
Incorrect Authorization	27-02-2020	10	DVR firmware in TAT-76 and TAT-77 series of products, provided by TONNET, contain misconfigured authentication mechanism. Attackers can crack the default password and gain access to the system.	<a href="https://tvn.twcert.org.tw/taiwanvn/TVN-201910003">https://tvn.twcert.org.tw/taiwanvn/TVN-201910003</a> , <a href="https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2b-bcf">https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2b-bcf</a>	H-TON-TAT--050320/815

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-3923</b>	8dd7-ec7213e2b bcf	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	27-02-2020	10	DVR firmware in TAT-76 and TAT-77 series of products, provided by TONNET do not properly verify patch files. Attackers can inject a specific command into a patch file and gain access to the system. <b>CVE ID : CVE-2020-3924</b>	<a href="https://tvn.twcert.org.tw/taiwanvn/TVN-201910004">https://tvn.twcert.org.tw/taiwanvn/TVN-201910004</a> , <a href="https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2b bcf">https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2b bcf</a>	H-TON-TAT--050320/816
<b>tat-76132g3</b>					
Incorrect Authorization	27-02-2020	10	DVR firmware in TAT-76 and TAT-77 series of products, provided by TONNET, contain misconfigured authentication mechanism. Attackers can crack the default password and gain access to the system. <b>CVE ID : CVE-2020-3923</b>	<a href="https://tvn.twcert.org.tw/taiwanvn/TVN-201910003">https://tvn.twcert.org.tw/taiwanvn/TVN-201910003</a> , <a href="https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2b bcf">https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2b bcf</a>	H-TON-TAT--050320/817
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	27-02-2020	10	DVR firmware in TAT-76 and TAT-77 series of products, provided by TONNET do not properly verify patch files. Attackers can inject a specific command into a patch file and gain access to the system.	<a href="https://tvn.twcert.org.tw/taiwanvn/TVN-201910004">https://tvn.twcert.org.tw/taiwanvn/TVN-201910004</a> , <a href="https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2b bcf">https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2b bcf</a>	H-TON-TAT--050320/818

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-3924</b>	8dd7-ec7213e2b bcf	
<b>tat-77104g1</b>					
Incorrect Authorization	27-02-2020	10	DVR firmware in TAT-76 and TAT-77 series of products, provided by TONNET, contain misconfigured authentication mechanism. Attackers can crack the default password and gain access to the system. <b>CVE ID : CVE-2020-3923</b>	<a href="https://tvn.twcert.org.tw/taiwanvn/TVN-201910003">https://tvn.twcert.org.tw/taiwanvn/TVN-201910003</a> , <a href="https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2b bcf">https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2b bcf</a>	H-TON-TAT--050320/819
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	27-02-2020	10	DVR firmware in TAT-76 and TAT-77 series of products, provided by TONNET do not properly verify patch files. Attackers can inject a specific command into a patch file and gain access to the system. <b>CVE ID : CVE-2020-3924</b>	<a href="https://tvn.twcert.org.tw/taiwanvn/TVN-201910004">https://tvn.twcert.org.tw/taiwanvn/TVN-201910004</a> , <a href="https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2b bcf">https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2b bcf</a>	H-TON-TAT--050320/820
<b>Tp-link</b>					
<b>tl-wr849n</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS	24-02-2020	7.5	On TP-Link TL-WR849N 0.9.1 4.16 devices, a remote command execution vulnerability in the diagnostics area can be exploited when an attacker sends specific shell	N/A	H-TP--TL-W-050320/821

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			metacharacters to the panel's traceroute feature. <b>CVE ID : CVE-2020-9374</b>		
<b>ZTE</b>					
<b>e8820v3</b>					
Incorrect Permission Assignment for Critical Resource	27-02-2020	3.3	ZTE E8820V3 router product is impacted by a permission and access control vulnerability. Attackers could use this vulnerability to tamper with DDNS parameters and send DoS attacks on the specified URL. <b>CVE ID : CVE-2020-6863</b>	<a href="http://support.zte.com.cn/support/news/Loo pholeInfoDetail.aspx?newsId=1012382">http://support.zte.com.cn/support/news/Loo pholeInfoDetail.aspx?newsId=1012382</a>	H-ZTE-E882-050320/822
Information Exposure	27-02-2020	3.3	ZTE E8820V3 router product is impacted by an information leak vulnerability. Attackers could use this vulnerability to to gain wireless passwords. After obtaining the wireless password, the attacker could collect information and attack the router. <b>CVE ID : CVE-2020-6864</b>	<a href="http://support.zte.com.cn/support/news/Loo pholeInfoDetail.aspx?newsId=1012382">http://support.zte.com.cn/support/news/Loo pholeInfoDetail.aspx?newsId=1012382</a>	H-ZTE-E882-050320/823
<b>Operating System</b>					
<b>abbott</b>					
<b>freestyle_libre_firmware</b>					
Out-of-bounds Write	16-02-2020	5.8	Older generation Abbott FreeStyle Libre sensors allow remote attackers within close proximity to enable write access to memory via a specific NFC unlock command. NOTE: The vulnerability is not present in the FreeStyle Libre 14-day	N/A	O-ABB-FREE-050320/824

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in the U.S (announced in August 2018) and FreeStyle Libre 2 outside the U.S (announced in October 2018). <b>CVE ID : CVE-2020-8997</b>		
<b>Apple</b>					
<b>iphone_os</b>					
Out-of-bounds Read	27-02-2020	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. Processing a maliciously crafted image may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3878</b>	N/A	O-APP-IPHO-050320/825
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted web content may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3825</b>	N/A	O-APP-IPHO-050320/826
Out-of-bounds Read	27-02-2020	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1,	N/A	O-APP-IPHO-050320/827

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			watchOS 6.1.2, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing a maliciously crafted image may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3826</b>		
Information Exposure	27-02-2020	2.1	A lock screen issue allowed access to contacts on a locked device. This issue was addressed with improved state management. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1. A person with physical access to an iOS device may be able to access contacts from the lock screen. <b>CVE ID : CVE-2020-3828</b>	N/A	O-APP-IPHO-050320/828
Out-of-bounds Read	27-02-2020	9.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An application may be able to gain elevated privileges. <b>CVE ID : CVE-2020-3829</b>	N/A	O-APP-IPHO-050320/829
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	27-02-2020	7.6	A race condition was addressed with improved locking. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1. An application may be able to execute arbitrary code with kernel privileges. <b>CVE ID : CVE-2020-3831</b>	N/A	O-APP-IPHO-050320/830

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	2.1	An access issue was addressed with improved memory management. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. A malicious application may be able to determine kernel memory layout. <b>CVE ID : CVE-2020-3836</b>	N/A	O-APP-IPHO-050320/831
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An application may be able to execute arbitrary code with kernel privileges. <b>CVE ID : CVE-2020-3837</b>	N/A	O-APP-IPHO-050320/832
Incorrect Default Permissions	27-02-2020	9.3	The issue was addressed with improved permissions logic. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An application may be able to execute arbitrary code with system privileges. <b>CVE ID : CVE-2020-3838</b>	N/A	O-APP-IPHO-050320/833
Improper Restriction of Operations within the Bounds of a Memory	27-02-2020	6.8	An off by one issue existed in the handling of racoon configuration files. This issue was addressed through improved bounds checking. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1,	N/A	O-APP-IPHO-050320/834

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			macOS Catalina 10.15.3, tvOS 13.3.1. Loading a maliciously crafted racoon configuration file may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3840</b>		
Insufficiently Protected Credentials	27-02-2020	4.3	The issue was addressed with improved UI handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, Safari 13.0.5. A local user may unknowingly send a password unencrypted over the network. <b>CVE ID : CVE-2020-3841</b>	N/A	O-APP-IPHO-050320/835
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An application may be able to execute arbitrary code with kernel privileges. <b>CVE ID : CVE-2020-3842</b>	N/A	O-APP-IPHO-050320/836
Incorrect Authorization	27-02-2020	2.1	This issue was addressed with improved checks. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1. Users removed from an iMessage conversation may still be able to alter state. <b>CVE ID : CVE-2020-3844</b>	N/A	O-APP-IPHO-050320/837
XML Injection (aka Blind XPath	27-02-2020	6.8	A buffer overflow was addressed with improved size validation. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS	N/A	O-APP-IPHO-050320/838

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection)			Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted XML may lead to an unexpected application termination or arbitrary code execution. <b>CVE ID : CVE-2020-3846</b>		
Access of Resource Using Incompatible Type ('Type Confusion')	27-02-2020	9.3	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. A malicious application may be able to execute arbitrary code with system privileges. <b>CVE ID : CVE-2020-3853</b>	N/A	O-APP-IPHO-050320/839
Improper Input Validation	27-02-2020	9.3	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. Processing a maliciously crafted string may lead to heap corruption. <b>CVE ID : CVE-2020-3856</b>	N/A	O-APP-IPHO-050320/840
Improper Restriction of Operations within the Bounds of a Memory	27-02-2020	7.2	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An	N/A	O-APP-IPHO-050320/841

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			application may be able to execute arbitrary code with system privileges. <b>CVE ID : CVE-2020-3857</b>		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1. An application may be able to execute arbitrary code with kernel privileges. <b>CVE ID : CVE-2020-3858</b>	N/A	O-APP-IPHO-050320/842
Information Exposure	27-02-2020	2.1	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1. A person with physical access to an iOS device may be able to access contacts from the lock screen. <b>CVE ID : CVE-2020-3859</b>	N/A	O-APP-IPHO-050320/843
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	7.2	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, watchOS 6.1.2. An application may be able to execute arbitrary code with kernel privileges. <b>CVE ID : CVE-2020-3860</b>	N/A	O-APP-IPHO-050320/844
Improper Restriction of Operations within the	27-02-2020	4.3	A denial of service issue was addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1,	N/A	O-APP-IPHO-050320/845

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. A malicious website may be able to cause a denial of service. <b>CVE ID : CVE-2020-3862</b>		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted web content may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3865</b>	N/A	O-APP-IPHO-050320/846
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-02-2020	4.3	A logic issue was addressed with improved state management. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted web content may lead to universal cross site scripting. <b>CVE ID : CVE-2020-3867</b>	N/A	O-APP-IPHO-050320/847
Improper Restriction of Operations within the	27-02-2020	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1,	N/A	O-APP-IPHO-050320/848

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted web content may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3868</b>		
N/A	27-02-2020	5	An issue existed in the handling of the local user's self-view. The issue was corrected with improved logic. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1. A remote FaceTime user may be able to cause the local user's camera self-view to display the incorrect camera. <b>CVE ID : CVE-2020-3869</b>	N/A	O-APP-IPHO-050320/849
Out-of-bounds Read	27-02-2020	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. Processing a maliciously crafted image may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3870</b>	N/A	O-APP-IPHO-050320/850
Improper Restriction of Operations within the Bounds of a Memory	27-02-2020	4.3	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An	N/A	O-APP-IPHO-050320/851

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			application may be able to read restricted memory. <b>CVE ID : CVE-2020-3872</b>		
Incorrect Authorization	27-02-2020	2.1	This issue was addressed with improved setting propagation. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1. Turning off "Load remote content in messages" may not apply to all mail previews. <b>CVE ID : CVE-2020-3873</b>	N/A	O-APP-IPHO-050320/852
Information Exposure	27-02-2020	5	An issued existed in the naming of screenshots. The issue was corrected with improved naming. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1. Screenshots of the Messages app may reveal additional message content. <b>CVE ID : CVE-2020-3874</b>	N/A	O-APP-IPHO-050320/853
Out-of-bounds Read	27-02-2020	4.3	A validation issue was addressed with improved input sanitization. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An application may be able to read restricted memory. <b>CVE ID : CVE-2020-3875</b>	N/A	O-APP-IPHO-050320/854
<b>mac_os_x</b>					
Out-of-bounds Read	27-02-2020	5	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.3, watchOS 6.1.2. A	N/A	O-APP-MAC_-050320/855

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attacker may be able to cause unexpected application termination or arbitrary code execution. <b>CVE ID : CVE-2020-3877</b>		
Out-of-bounds Read	27-02-2020	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. Processing a maliciously crafted image may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3878</b>	N/A	O-APP-MAC_-050320/856
Out-of-bounds Read	27-02-2020	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing a maliciously crafted image may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3826</b>	N/A	O-APP-MAC_-050320/857
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	9.3	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.3. Viewing a maliciously crafted JPEG file may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3827</b>	N/A	O-APP-MAC_-050320/858

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	27-02-2020	9.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An application may be able to gain elevated privileges. <b>CVE ID : CVE-2020-3829</b>	N/A	O-APP-MAC_-050320/859
Improper Link Resolution Before File Access ('Link Following')	27-02-2020	3.6	A validation issue existed in the handling of symlinks. This issue was addressed with improved validation of symlinks. This issue is fixed in macOS Catalina 10.15.3. A malicious application may be able to overwrite arbitrary files. <b>CVE ID : CVE-2020-3830</b>	N/A	O-APP-MAC_-050320/860
Improper Link Resolution Before File Access ('Link Following')	27-02-2020	3.6	A validation issue existed in the handling of symlinks. This issue was addressed with improved validation of symlinks. This issue is fixed in macOS Catalina 10.15.3. A malicious application may be able to access restricted files. <b>CVE ID : CVE-2020-3835</b>	N/A	O-APP-MAC_-050320/861
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	2.1	An access issue was addressed with improved memory management. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. A malicious application may be able to determine kernel memory layout.	N/A	O-APP-MAC_-050320/862

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-3836</b>		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An application may be able to execute arbitrary code with kernel privileges. <b>CVE ID : CVE-2020-3837</b>	N/A	O-APP-MAC_-050320/863
Incorrect Default Permissions	27-02-2020	9.3	The issue was addressed with improved permissions logic. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An application may be able to execute arbitrary code with system privileges. <b>CVE ID : CVE-2020-3838</b>	N/A	O-APP-MAC_-050320/864
Improper Input Validation	27-02-2020	2.1	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Catalina 10.15.3. An application may be able to read restricted memory. <b>CVE ID : CVE-2020-3839</b>	N/A	O-APP-MAC_-050320/865
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	6.8	An off by one issue existed in the handling of racoon configuration files. This issue was addressed through improved bounds checking. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1. Loading a maliciously	N/A	O-APP-MAC_-050320/866

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted racoon configuration file may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3840</b>		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An application may be able to execute arbitrary code with kernel privileges. <b>CVE ID : CVE-2020-3842</b>	N/A	O-APP-MAC_-050320/867
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	9.3	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.3. A remote attacker may be able to cause unexpected system termination or corrupt kernel memory. <b>CVE ID : CVE-2020-3843</b>	N/A	O-APP-MAC_-050320/868
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15.3. An application may be able to execute arbitrary code with system privileges. <b>CVE ID : CVE-2020-3845</b>	N/A	O-APP-MAC_-050320/869
XML Injection (aka Blind XPath)	27-02-2020	6.8	A buffer overflow was addressed with improved size validation. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS	N/A	O-APP-MAC_-050320/870

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection)			Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted XML may lead to an unexpected application termination or arbitrary code execution. <b>CVE ID : CVE-2020-3846</b>		
Access of Resource Using Incompatible Type ('Type Confusion')	27-02-2020	9.3	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. A malicious application may be able to execute arbitrary code with system privileges. <b>CVE ID : CVE-2020-3853</b>	N/A	O-APP-MAC_-050320/871
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15.3. An application may be able to execute arbitrary code with system privileges. <b>CVE ID : CVE-2020-3854</b>	N/A	O-APP-MAC_-050320/872
Improper Input Validation	27-02-2020	9.3	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. Processing a maliciously crafted string may lead to	N/A	O-APP-MAC_-050320/873

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			heap corruption. <b>CVE ID : CVE-2020-3856</b>		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	7.2	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An application may be able to execute arbitrary code with system privileges. <b>CVE ID : CVE-2020-3857</b>	N/A	O-APP-MAC_-050320/874
Incorrect Authorization	27-02-2020	4.3	This was addressed with additional checks by Gatekeeper on files mounted through a network share. This issue is fixed in macOS Catalina 10.15.3. Searching for and opening a file from an attacker controlled NFS mount may bypass Gatekeeper. <b>CVE ID : CVE-2020-3866</b>	N/A	O-APP-MAC_-050320/875
Out-of-bounds Read	27-02-2020	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. Processing a maliciously crafted image may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3870</b>	N/A	O-APP-MAC_-050320/876
Improper Restriction of Operations	27-02-2020	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS	N/A	O-APP-MAC_-050320/877

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Catalina 10.15.3. An application may be able to execute arbitrary code with kernel privileges. <b>CVE ID : CVE-2020-3871</b>		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	4.3	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An application may be able to read restricted memory. <b>CVE ID : CVE-2020-3872</b>	N/A	O-APP-MAC_-050320/878
Out-of-bounds Read	27-02-2020	4.3	A validation issue was addressed with improved input sanitization. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An application may be able to read restricted memory. <b>CVE ID : CVE-2020-3875</b>	N/A	O-APP-MAC_-050320/879
<b>watchos</b>					
Out-of-bounds Read	27-02-2020	5	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.3, watchOS 6.1.2. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. <b>CVE ID : CVE-2020-3877</b>	N/A	O-APP-WATC-050320/880
Out-of-bounds Read	27-02-2020	6.8	An out-of-bounds read was addressed with improved	N/A	O-APP-WATC-050320/881

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input validation. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. Processing a maliciously crafted image may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3878</b>		
Out-of-bounds Read	27-02-2020	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing a maliciously crafted image may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3826</b>	N/A	O-APP-WATC-050320/882
Out-of-bounds Read	27-02-2020	9.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An application may be able to gain elevated privileges. <b>CVE ID : CVE-2020-3829</b>	N/A	O-APP-WATC-050320/883
Improper Restriction of Operations within the Bounds of a	27-02-2020	9.3	A memory corruption issue was addressed with improved state management. This issue is fixed in watchOS 6.1.2. An application may be able to	N/A	O-APP-WATC-050320/884

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			execute arbitrary code with kernel privileges. <b>CVE ID : CVE-2020-3834</b>		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	2.1	An access issue was addressed with improved memory management. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. A malicious application may be able to determine kernel memory layout. <b>CVE ID : CVE-2020-3836</b>	N/A	O-APP-WATC-050320/885
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An application may be able to execute arbitrary code with kernel privileges. <b>CVE ID : CVE-2020-3837</b>	N/A	O-APP-WATC-050320/886
Incorrect Default Permissions	27-02-2020	9.3	The issue was addressed with improved permissions logic. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An application may be able to execute arbitrary code with system privileges. <b>CVE ID : CVE-2020-3838</b>	N/A	O-APP-WATC-050320/887
Improper Restriction of Operations	27-02-2020	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS	N/A	O-APP-WATC-050320/888

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An application may be able to execute arbitrary code with kernel privileges. <b>CVE ID : CVE-2020-3842</b>		
XML Injection (aka Blind XPath Injection)	27-02-2020	6.8	A buffer overflow was addressed with improved size validation. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted XML may lead to an unexpected application termination or arbitrary code execution. <b>CVE ID : CVE-2020-3846</b>	N/A	O-APP-WATC-050320/889
Access of Resource Using Incompatible Type ('Type Confusion')	27-02-2020	9.3	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. A malicious application may be able to execute arbitrary code with system privileges. <b>CVE ID : CVE-2020-3853</b>	N/A	O-APP-WATC-050320/890
Improper Input Validation	27-02-2020	9.3	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS	N/A	O-APP-WATC-050320/891

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			13.3.1, watchOS 6.1.2. Processing a maliciously crafted string may lead to heap corruption. <b>CVE ID : CVE-2020-3856</b>		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	7.2	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An application may be able to execute arbitrary code with system privileges. <b>CVE ID : CVE-2020-3857</b>	N/A	O-APP-WATC-050320/892
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	7.2	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, watchOS 6.1.2. An application may be able to execute arbitrary code with kernel privileges. <b>CVE ID : CVE-2020-3860</b>	N/A	O-APP-WATC-050320/893
Out-of-bounds Read	27-02-2020	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. Processing a maliciously crafted image may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3870</b>	N/A	O-APP-WATC-050320/894
Improper Restriction	27-02-2020	4.3	A memory initialization issue was addressed with	N/A	O-APP-WATC-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An application may be able to read restricted memory. <b>CVE ID : CVE-2020-3872</b>		050320/895
Out-of-bounds Read	27-02-2020	4.3	A validation issue was addressed with improved input sanitization. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An application may be able to read restricted memory. <b>CVE ID : CVE-2020-3875</b>	N/A	O-APP-WATC-050320/896
<b>tvos</b>					
Out-of-bounds Read	27-02-2020	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. Processing a maliciously crafted image may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3878</b>	N/A	O-APP-TVOS-050320/897
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17.	N/A	O-APP-TVOS-050320/898

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processing maliciously crafted web content may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3825</b>		
Out-of-bounds Read	27-02-2020	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing a maliciously crafted image may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3826</b>	N/A	O-APP-TVOS-050320/899
Out-of-bounds Read	27-02-2020	9.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An application may be able to gain elevated privileges. <b>CVE ID : CVE-2020-3829</b>	N/A	O-APP-TVOS-050320/900
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	2.1	An access issue was addressed with improved memory management. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. A malicious application may be able to determine kernel memory layout.	N/A	O-APP-TVOS-050320/901

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-3836</b>		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An application may be able to execute arbitrary code with kernel privileges. <b>CVE ID : CVE-2020-3837</b>	N/A	O-APP-TVOS-050320/902
Incorrect Default Permissions	27-02-2020	9.3	The issue was addressed with improved permissions logic. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An application may be able to execute arbitrary code with system privileges. <b>CVE ID : CVE-2020-3838</b>	N/A	O-APP-TVOS-050320/903
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	6.8	An off by one issue existed in the handling of racoon configuration files. This issue was addressed through improved bounds checking. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1. Loading a maliciously crafted racoon configuration file may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3840</b>	N/A	O-APP-TVOS-050320/904
Improper Restriction of Operations	27-02-2020	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS	N/A	O-APP-TVOS-050320/905

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An application may be able to execute arbitrary code with kernel privileges. <b>CVE ID : CVE-2020-3842</b>		
XML Injection (aka Blind XPath Injection)	27-02-2020	6.8	A buffer overflow was addressed with improved size validation. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted XML may lead to an unexpected application termination or arbitrary code execution. <b>CVE ID : CVE-2020-3846</b>	N/A	O-APP-TVOS-050320/906
Access of Resource Using Incompatible Type ('Type Confusion')	27-02-2020	9.3	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. A malicious application may be able to execute arbitrary code with system privileges. <b>CVE ID : CVE-2020-3853</b>	N/A	O-APP-TVOS-050320/907
Improper Input Validation	27-02-2020	9.3	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS	N/A	O-APP-TVOS-050320/908

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			13.3.1, watchOS 6.1.2. Processing a maliciously crafted string may lead to heap corruption. <b>CVE ID : CVE-2020-3856</b>		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	7.2	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An application may be able to execute arbitrary code with system privileges. <b>CVE ID : CVE-2020-3857</b>	N/A	O-APP-TVOS-050320/909
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	4.3	A denial of service issue was addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. A malicious website may be able to cause a denial of service. <b>CVE ID : CVE-2020-3862</b>	N/A	O-APP-TVOS-050320/910
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted web content may	N/A	O-APP-TVOS-050320/911

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to arbitrary code execution. <b>CVE ID : CVE-2020-3865</b>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-02-2020	4.3	A logic issue was addressed with improved state management. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted web content may lead to universal cross site scripting. <b>CVE ID : CVE-2020-3867</b>	N/A	O-APP-TVOS-050320/912
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted web content may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3868</b>	N/A	O-APP-TVOS-050320/913
Out-of-bounds Read	27-02-2020	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. Processing a maliciously crafted image may lead to arbitrary code	N/A	O-APP-TVOS-050320/914

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. <b>CVE ID : CVE-2020-3870</b>		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	4.3	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An application may be able to read restricted memory. <b>CVE ID : CVE-2020-3872</b>	N/A	O-APP-TVOS-050320/915
Out-of-bounds Read	27-02-2020	4.3	A validation issue was addressed with improved input sanitization. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An application may be able to read restricted memory. <b>CVE ID : CVE-2020-3875</b>	N/A	O-APP-TVOS-050320/916
<b>ipados</b>					
Out-of-bounds Read	27-02-2020	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. Processing a maliciously crafted image may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3878</b>	N/A	O-APP-IPAD-050320/917
Improper Restriction of Operations	27-02-2020	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS	N/A	O-APP-IPAD-050320/918

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted web content may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3825</b>		
Out-of-bounds Read	27-02-2020	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing a maliciously crafted image may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3826</b>	N/A	O-APP-IPAD-050320/919
Information Exposure	27-02-2020	2.1	A lock screen issue allowed access to contacts on a locked device. This issue was addressed with improved state management. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1. A person with physical access to an iOS device may be able to access contacts from the lock screen. <b>CVE ID : CVE-2020-3828</b>	N/A	O-APP-IPAD-050320/920
Out-of-bounds Read	27-02-2020	9.3	An out-of-bounds read was addressed with improved bounds checking. This issue	N/A	O-APP-IPAD-050320/921

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An application may be able to gain elevated privileges. <b>CVE ID : CVE-2020-3829</b>		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	27-02-2020	7.6	A race condition was addressed with improved locking. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1. An application may be able to execute arbitrary code with kernel privileges. <b>CVE ID : CVE-2020-3831</b>	N/A	O-APP-IPAD-050320/922
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	2.1	An access issue was addressed with improved memory management. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. A malicious application may be able to determine kernel memory layout. <b>CVE ID : CVE-2020-3836</b>	N/A	O-APP-IPAD-050320/923
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An application may be able to execute arbitrary code with kernel privileges. <b>CVE ID : CVE-2020-3837</b>	N/A	O-APP-IPAD-050320/924
Incorrect	27-02-2020	9.3	The issue was addressed	N/A	O-APP-IPAD-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Default Permissions			with improved permissions logic. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An application may be able to execute arbitrary code with system privileges. <b>CVE ID : CVE-2020-3838</b>		050320/925
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	6.8	An off by one issue existed in the handling of racoon configuration files. This issue was addressed through improved bounds checking. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1. Loading a maliciously crafted racoon configuration file may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3840</b>	N/A	O-APP-IPAD-050320/926
Insufficiently Protected Credentials	27-02-2020	4.3	The issue was addressed with improved UI handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, Safari 13.0.5. A local user may unknowingly send a password unencrypted over the network. <b>CVE ID : CVE-2020-3841</b>	N/A	O-APP-IPAD-050320/927
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An application may be able to	N/A	O-APP-IPAD-050320/928

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code with kernel privileges. <b>CVE ID : CVE-2020-3842</b>		
Incorrect Authorization	27-02-2020	2.1	This issue was addressed with improved checks. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1. Users removed from an iMessage conversation may still be able to alter state. <b>CVE ID : CVE-2020-3844</b>	N/A	O-APP-IPAD-050320/929
XML Injection (aka Blind XPath Injection)	27-02-2020	6.8	A buffer overflow was addressed with improved size validation. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted XML may lead to an unexpected application termination or arbitrary code execution. <b>CVE ID : CVE-2020-3846</b>	N/A	O-APP-IPAD-050320/930
Access of Resource Using Incompatible Type ('Type Confusion')	27-02-2020	9.3	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. A malicious application may be able to execute arbitrary code with system privileges. <b>CVE ID : CVE-2020-3853</b>	N/A	O-APP-IPAD-050320/931
Improper Input	27-02-2020	9.3	A memory corruption issue was addressed with	N/A	O-APP-IPAD-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			improved input validation. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. Processing a maliciously crafted string may lead to heap corruption. <b>CVE ID : CVE-2020-3856</b>		050320/932
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	7.2	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An application may be able to execute arbitrary code with system privileges. <b>CVE ID : CVE-2020-3857</b>	N/A	O-APP-IPAD-050320/933
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1. An application may be able to execute arbitrary code with kernel privileges. <b>CVE ID : CVE-2020-3858</b>	N/A	O-APP-IPAD-050320/934
Information Exposure	27-02-2020	2.1	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1. A person with physical access to an iOS device may be able to access contacts from the lock screen.	N/A	O-APP-IPAD-050320/935

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-3859</b>		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	7.2	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, watchOS 6.1.2. An application may be able to execute arbitrary code with kernel privileges. <b>CVE ID : CVE-2020-3860</b>	N/A	O-APP-IPAD-050320/936
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	4.3	A denial of service issue was addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. A malicious website may be able to cause a denial of service. <b>CVE ID : CVE-2020-3862</b>	N/A	O-APP-IPAD-050320/937
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted web content may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3865</b>	N/A	O-APP-IPAD-050320/938
Improper Neutralization	27-02-2020	4.3	A logic issue was addressed with improved state	N/A	O-APP-IPAD-050320/939

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			management. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted web content may lead to universal cross site scripting. <b>CVE ID : CVE-2020-3867</b>		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted web content may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3868</b>	N/A	O-APP-IPAD-050320/940
N/A	27-02-2020	5	An issue existed in the handling of the local user's self-view. The issue was corrected with improved logic. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1. A remote FaceTime user may be able to cause the local user's camera self-view to display the incorrect camera. <b>CVE ID : CVE-2020-3869</b>	N/A	O-APP-IPAD-050320/941
Out-of-bounds Read	27-02-2020	6.8	An out-of-bounds read was addressed with improved	N/A	O-APP-IPAD-050320/942

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input validation. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. Processing a maliciously crafted image may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3870</b>		
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	4.3	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An application may be able to read restricted memory. <b>CVE ID : CVE-2020-3872</b>	N/A	O-APP-IPAD-050320/943
Incorrect Authorization	27-02-2020	2.1	This issue was addressed with improved setting propagation. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1. Turning off "Load remote content in messages" may not apply to all mail previews. <b>CVE ID : CVE-2020-3873</b>	N/A	O-APP-IPAD-050320/944
Information Exposure	27-02-2020	5	An issued existed in the naming of screenshots. The issue was corrected with improved naming. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1. Screenshots of the Messages app may reveal additional message content. <b>CVE ID : CVE-2020-3874</b>	N/A	O-APP-IPAD-050320/945

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	27-02-2020	4.3	A validation issue was addressed with improved input sanitization. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, macOS Catalina 10.15.3, tvOS 13.3.1, watchOS 6.1.2. An application may be able to read restricted memory. <b>CVE ID : CVE-2020-3875</b>	N/A	O-APP-IPAD-050320/946
<b>cambiumnetworks</b>					
<b>xh2-120_firmware</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-02-2020	4.3	An issue was discovered on Xirrus XR520, XR620, XR2436, and XH2-120 devices. The cgi-bin/ViewPage.cgi user parameter allows XSS. <b>CVE ID : CVE-2020-9022</b>	N/A	O-CAM-XH2--050320/947
<b>xr2436_firmware</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-02-2020	4.3	An issue was discovered on Xirrus XR520, XR620, XR2436, and XH2-120 devices. The cgi-bin/ViewPage.cgi user parameter allows XSS. <b>CVE ID : CVE-2020-9022</b>	N/A	O-CAM-XR24-050320/948
<b>xr520_firmware</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-02-2020	4.3	An issue was discovered on Xirrus XR520, XR620, XR2436, and XH2-120 devices. The cgi-bin/ViewPage.cgi user parameter allows XSS. <b>CVE ID : CVE-2020-9022</b>	N/A	O-CAM-XR52-050320/949

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<b>xr620_firmware</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-02-2020	4.3	An issue was discovered on Xirrus XR520, XR620, XR2436, and XH2-120 devices. The cgi-bin/ViewPage.cgi user parameter allows XSS. <b>CVE ID : CVE-2020-9022</b>	N/A	O-CAM-XR62-050320/950
<b>Cisco</b>					
<b>fxos</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	A vulnerability in the CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS). The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges. <b>CVE ID : CVE-2020-3167</b>	N/A	O-CIS-FXOS-050320/951

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	<p>A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying Linux operating system with a privilege level of root on an affected device. The vulnerability is due to insufficient validation of arguments passed to a specific CLI command on the affected device. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system with root privileges. An attacker would need valid administrator credentials to exploit this vulnerability.</p> <p><b>CVE ID : CVE-2020-3169</b></p>	N/A	O-CIS-FXOS-050320/952
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-02-2020	7.2	<p>A vulnerability in the local management (local-mgmt) CLI of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) of an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit</p>	N/A	O-CIS-FXOS-050320/953

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>this vulnerability by including crafted arguments to specific commands. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS with the privileges of the currently logged-in user for all affected platforms excluding Cisco UCS 6400 Series Fabric Interconnects. On Cisco UCS 6400 Series Fabric Interconnects, the injected commands are executed with root privileges.</p> <p><b>CVE ID : CVE-2020-3171</b></p>		
<b>nx-os</b>					
Improper Input Validation	26-02-2020	4.3	<p>A vulnerability in the NX-API feature of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause an NX-API system process to unexpectedly restart. The vulnerability is due to incorrect validation of the HTTP header of a request that is sent to the NX-API. An attacker could exploit this vulnerability by sending a crafted HTTP request to the NX-API on an affected device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition in the NX-API service; however, the Cisco NX-OS device itself would still be available and</p>	N/A	O-CIS-NX-O-050320/954

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>passing network traffic.</p> <p>Note: The NX-API feature is disabled by default.</p> <p><b>CVE ID : CVE-2020-3170</b></p>		
Insufficient Verification of Data Authenticity	26-02-2020	3.3	<p>A vulnerability in the anycast gateway feature of Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a device to learn invalid Address Resolution Protocol (ARP) entries. The ARP entries are for nonlocal IP addresses for the subnet. The vulnerability is due to improper validation of a received gratuitous ARP (GARP) request. An attacker could exploit this vulnerability by sending a malicious GARP packet on the local subnet to cause the ARP table on the device to become corrupted. A successful exploit could allow the attacker to populate the ARP table with incorrect entries, which could lead to traffic disruptions.</p> <p><b>CVE ID : CVE-2020-3174</b></p>	N/A	O-CIS-NX-O-050320/955
Uncontrolled Resource Consumption	26-02-2020	7.8	<p>A vulnerability in the resource handling system of Cisco NX-OS Software for Cisco MDS 9000 Series Multilayer Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected</p>	N/A	O-CIS-NX-O-050320/956

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. The vulnerability is due to improper resource usage control. An attacker could exploit this vulnerability by sending traffic to the management interface (mgmt0) of an affected device at very high rates. An exploit could allow the attacker to cause unexpected behaviors such as high CPU usage, process crashes, or even full system reboots of an affected device. <b>CVE ID : CVE-2020-3175</b>		
<b>Dell</b>					
<b>g3_15_3590_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	O-DEL-G3_1-050320/957
<b>g5_15_5590_firmware</b>					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.  <b>CVE ID : CVE-2020-5324</b>	N/A	O-DEL-G5_1-050320/958
<b>g5_5090_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload	N/A	O-DEL-G5_5-050320/959

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>		
<b>g7_15_7590_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	O-DEL-G7_1-050320/960
<b>g7_17_7790_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking	N/A	O-DEL-G7_1-050320/961

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>		
<b>inspiron_14_5490_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	O-DEL-INSP-050320/962
<b>inspiron_3490_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an	N/A	O-DEL-INSP-050320/963

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
<b>inspiron_3493_firmware</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	O-DEL-INSP-050320/964
<b>inspiron_3590_firmware</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File</p>	N/A	O-DEL-INSP-050320/965

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
<b>inspiron_3593_firmware</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	O-DEL-INSP-050320/966

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<b>inspiron_3790_firmware</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	O-DEL-INSP-050320/967
<b>inspiron_3793_firmware</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect</p>	N/A	O-DEL-INSP-050320/968

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>		
<b>inspiron_5390_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	O-DEL-INSP-050320/969
<b>inspiron_5391_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit	N/A	O-DEL-INSP-050320/970

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>		
<b>inspiron_5491_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	O-DEL-INSP-050320/971
<b>inspiron_5493_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window	N/A	O-DEL-INSP-050320/972

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
<b>inspiron_5494_firmware</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	O-DEL-INSP-050320/973
<b>inspiron_5498_firmware</b>					
Improper Input	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms	N/A	O-DEL-INSP-050320/974

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			<p>contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
<b>inspiron_5583_firmware</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p>	N/A	O-DEL-INSP-050320/975

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-5324</b>		
<b>inspiron_5584_firmware</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	O-DEL-INSP-050320/976
<b>inspiron_5590_firmware</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The</p>	N/A	O-DEL-INSP-050320/977

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>		
<b>inspiron_5591_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	O-DEL-INSP-050320/978
<b>inspiron_5593_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged	N/A	O-DEL-INSP-050320/979

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>		
<b>inspiron_5594_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	O-DEL-INSP-050320/980
<b>inspiron_5598_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility	N/A	O-DEL-INSP-050320/981

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
<b>inspiron_7390_firmware</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	O-DEL-INSP-050320/982
<b>inspiron_7391_firmware</b>					
Improper	21-02-2020	2.6	Dell Client Consumer and	N/A	O-DEL-INSP-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.  <b>CVE ID : CVE-2020-5324</b>		050320/983
<b>inspiron_7490_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility	N/A	O-DEL-INSP-050320/984

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			delivers. <b>CVE ID : CVE-2020-5324</b>		
<b>inspiron_7590_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	O-DEL-INSP-050320/985
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-	N/A	O-DEL-INSP-050320/986

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>inspiron_7591_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	O-DEL-INSP-050320/987
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-	N/A	O-DEL-INSP-050320/988

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>inspiron_7791_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	O-DEL-INSP-050320/989
<b>latitude_3301_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into	N/A	O-DEL-LATI-050320/990

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>		
<b>latitude_3300_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	O-DEL-LATI-050320/991
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the	N/A	O-DEL-LATI-050320/992

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>latitude_3311_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	O-DEL-LATI-050320/993
<b>latitude_3400_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this	N/A	O-DEL-LATI-050320/994

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>		
<b>latitude_3500_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	O-DEL-LATI-050320/995
<b>latitude_5300_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The	N/A	O-DEL-LATI-050320/996

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	O-DEL-LATI-050320/997
<b>latitude_5400_firmware</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The</p>	N/A	O-DEL-LATI-050320/998

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	O-DEL-LATI-050320/999
<b>latitude_5401_firmware</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The</p>	N/A	O-DEL-LATI-050320/1000

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	O-DEL-LATI-050320/1001
<b>latitude_5420_rugged_firmware</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The</p>	N/A	O-DEL-LATI-050320/1002

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	O-DEL-LATI-050320/1003
<b>latitude_5424_rugged_firmware</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The</p>	N/A	O-DEL-LATI-050320/1004

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	O-DEL-LATI-050320/1005
<b>latitude_5500_firmware</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The</p>	N/A	O-DEL-LATI-050320/1006

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	O-DEL-LATI-050320/1007
<b>latitude_5501_firmware</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The</p>	N/A	O-DEL-LATI-050320/1008

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	O-DEL-LATI-050320/1009
<b>latitude_7200_firmware</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The</p>	N/A	O-DEL-LATI-050320/1010

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
<b>latitude_7220_rugged_extreme_tablet_firmware</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	O-DEL-LATI-050320/1011

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<b>latitude_7220ex_rugged_extreme_tablet_firmware</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	O-DEL-LATI-050320/1012
<b>latitude_7300_firmware</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect</p>	N/A	O-DEL-LATI-050320/1013

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>		
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-LATI-050320/1014
<b>latitude_7400_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect	N/A	O-DEL-LATI-050320/1015

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>		
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-LATI-050320/1016
<b>precision_3540_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect	N/A	O-DEL-PREC-050320/1017

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>		
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-PREC-050320/1018
<b>precision_3541_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect	N/A	O-DEL-PREC-050320/1019

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>		
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-PREC-050320/1020
<b>precision_5540_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect	N/A	O-DEL-PREC-050320/1021

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>		
<b>precision_7540_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	O-DEL-PREC-050320/1022
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by	N/A	O-DEL-PREC-050320/1023

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>precision_7730_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	O-DEL-PREC-050320/1024
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by	N/A	O-DEL-PREC-050320/1025

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>precision_7740_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	O-DEL-PREC-050320/1026
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by	N/A	O-DEL-PREC-050320/1027

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>vostro_15_7580_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	O-DEL-VOST-050320/1028
<b>vostro_3481_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit	N/A	O-DEL-VOST-050320/1029

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>		
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-VOST-050320/1030
<b>vostro_3490_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit	N/A	O-DEL-VOST-050320/1031

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
<b>vostro_3590_firmware</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	O-DEL-VOST-050320/1032
<b>vostro_5390_firmware</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window</p>	N/A	O-DEL-VOST-050320/1033

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
<b>vostro_5391_firmware</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	O-DEL-VOST-050320/1034
<b>vostro_5490_firmware</b>					
Improper Input	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms	N/A	O-DEL-VOST-050320/1035

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			<p>contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
<b>vostro_5590_firmware</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p>	N/A	O-DEL-VOST-050320/1036

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-5324</b>		
<b>vostro_7590_firmware</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	O-DEL-VOST-050320/1037
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p>	N/A	O-DEL-VOST-050320/1038

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-5326</b>		
<b>wyse_5070_thin_client_firmware</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	O-DEL-WYSE-050320/1039
<b>wyse_5470_firmware</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The</p>	N/A	O-DEL-WYSE-050320/1040

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>		
<b>xps_13_9380_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	O-DEL-XPS_-050320/1041
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring	N/A	O-DEL-XPS_-050320/1042

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>xps_15_9575_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	O-DEL-XPS_-050320/1043
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring	N/A	O-DEL-XPS_-050320/1044

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>xps_15_7590_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	O-DEL-XPS_-050320/1045
<b>xps_15_9570_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged	N/A	O-DEL-XPS_-050320/1046

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>		
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-XPS_-050320/1047
<b>g3_3590_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the	N/A	O-DEL-G3_3-050320/1048

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>inspiron_14_gaming_7466_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-INSP-050320/1049
<b>inspiron_14_gaming_7467_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration	N/A	O-DEL-INSP-050320/1050

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>inspiron_15_7572_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-INSP-050320/1051
<b>inspiron_15_gaming_7566_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring	N/A	O-DEL-INSP-050320/1052

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>inspiron_15_gaming_7567_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-INSP-050320/1053
<b>inspiron_15_gaming_7577_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by	N/A	O-DEL-INSP-050320/1054

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>g7_7588_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	O-DEL-G7_7-050320/1055
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by	N/A	O-DEL-G7_7-050320/1056

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>latitude_3390_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	O-DEL-LATI-050320/1057
<b>latitude_3460_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration	N/A	O-DEL-LATI-050320/1058

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>latitude_3480_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-LATI-050320/1059
<b>latitude_3490_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking	N/A	O-DEL-LATI-050320/1060

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>		
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-LATI-050320/1061
latitude_3580_firmware					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring	N/A	O-DEL-LATI-050320/1062

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>latitude_3590_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	O-DEL-LATI-050320/1063
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring	N/A	O-DEL-LATI-050320/1064

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>latitude_5175_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-LATI-050320/1065
<b>latitude_5179_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by	N/A	O-DEL-LATI-050320/1066

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>latitude_5280_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-LATI-050320/1067
<b>latitude_5288_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized	N/A	O-DEL-LATI-050320/1068

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>latitude_5289_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-LATI-050320/1069
<b>latitude_5290_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The	N/A	O-DEL-LATI-050320/1070

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>		
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-LATI-050320/1071
latitude_5414_firmware					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-	N/A	O-DEL-LATI-050320/1072

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>latitude_5480_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-LATI-050320/1073
<b>latitude_5488_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.	N/A	O-DEL-LATI-050320/1074

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-5326</b>		
<b>latitude_5490_firmware</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	O-DEL-LATI-050320/1075
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p>	N/A	O-DEL-LATI-050320/1076

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-5326</b>		
<b>latitude_5491_firmware</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	O-DEL-LATI-050320/1077
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p>	N/A	O-DEL-LATI-050320/1078

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-5326</b>		
<b>precision_3630_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-PREC-050320/1079
<b>precision_3930_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-PREC-050320/1080

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<b>precision_5510_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.  <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-PREC-050320/1081
<b>precision_5520_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.  <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-PREC-050320/1082
<b>precision_5530_firmware</b>					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	O-DEL-PREC-050320/1083
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	O-DEL-PREC-050320/1084
precision_5820_firmware					

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-PREC-050320/1085
<b>precision_7510_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-PREC-050320/1086
<b>precision_7520_firmware</b>					
Missing	21-02-2020	2.1	Affected Dell Client	N/A	O-DEL-PREC-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication for Critical Function			platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		050320/1087
<b>precision_7530_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	O-DEL-PREC-050320/1088

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-PREC-050320/1089
<b>precision_7710_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-PREC-050320/1090
<b>precision_7720_firmware</b>					
Missing	21-02-2020	2.1	Affected Dell Client	N/A	O-DEL-PREC-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication for Critical Function			platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		050320/1091
<b>precision_7820_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-PREC-050320/1092
<b>precision_7920_firmware</b>					
Missing Authentication	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS	N/A	O-DEL-PREC-050320/1093

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on for Critical Function			Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>vostro_7580_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-VOST-050320/1094
<b>vostro_3070_firmware</b>					
Missing Authentication for	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration	N/A	O-DEL-VOST-050320/1095

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Critical Function			authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>chengming_3980_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-CHEN-050320/1096
<b>g3_3579_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The	N/A	O-DEL-G3_3-050320/1097

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	O-DEL-G3_3-050320/1098
<b>g5_5587_firmware</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The</p>	N/A	O-DEL-G5_5-050320/1099

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	O-DEL-G5_5-050320/1100
<b>g5_5590_firmware</b>					
Missing Authentication for Critical	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass</p>	N/A	O-DEL-G5_5-050320/1101

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Function			vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>g7_7790_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-G7_7-050320/1102
<b>xps_8900_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot	N/A	O-DEL-XPS_-050320/1103

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>g3_3779_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	O-DEL-G3_3-050320/1104
Missing Authentication for Critical	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot	N/A	O-DEL-G3_3-050320/1105

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Function			Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>g7_7590_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-G7_7-050320/1106
<b>embedded_box_pc_5000_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage	N/A	O-DEL-EMBE-050320/1107

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>latitude_5580_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-LATI-050320/1108
<b>latitude_5590_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window	N/A	O-DEL-LATI-050320/1109

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	O-DEL-LATI-050320/1110
latitude_5591_firmware					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window</p>	N/A	O-DEL-LATI-050320/1111

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	O-DEL-LATI-050320/1112
latitude_7202_firmware					
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST)</p>	N/A	O-DEL-LATI-050320/1113

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>latitude_7212_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-LATI-050320/1114
<b>latitude_7214_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker	N/A	O-DEL-LATI-050320/1115

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>latitude_7275_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-LATI-050320/1116
<b>latitude_7280_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the	N/A	O-DEL-LATI-050320/1117

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>latitude_7285_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-LATI-050320/1118
<b>latitude_7290_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally	N/A	O-DEL-LATI-050320/1119

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>		
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-LATI-050320/1120
latitude_7370_firmware					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform	N/A	O-DEL-LATI-050320/1121

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>latitude_7380_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-LATI-050320/1122
<b>latitude_7389_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the	N/A	O-DEL-LATI-050320/1123

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>latitude_7390_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	O-DEL-LATI-050320/1124
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the	N/A	O-DEL-LATI-050320/1125

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>latitude_7414_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-LATI-050320/1126
<b>latitude_7424_rugged_extreme_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit	N/A	O-DEL-LATI-050320/1127

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>		
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-LATI-050320/1128
<b>latitude_7480_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration	N/A	O-DEL-LATI-050320/1129

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>latitude_7490_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	O-DEL-LATI-050320/1130
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration	N/A	O-DEL-LATI-050320/1131

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>latitude_e5270_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-LATI-050320/1132
<b>latitude_e5470_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring	N/A	O-DEL-LATI-050320/1133

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>latitude_e5570_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-LATI-050320/1134
<b>latitude_e7270_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by	N/A	O-DEL-LATI-050320/1135

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>latitude_e7470_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-LATI-050320/1136
<b>optiplex_3040_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized	N/A	O-DEL-OPTI-050320/1137

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>optiplex_3046_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-OPTI-050320/1138
<b>optiplex_3050_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-	N/A	O-DEL-OPTI-050320/1139

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>optiplex_3060_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-OPTI-050320/1140
<b>optiplex_5040_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.	N/A	O-DEL-OPTI-050320/1141

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-5326</b>		
<b>optiplex_5050_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-OPTI-050320/1142
<b>optiplex_5060_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-OPTI-050320/1143

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<b>optiplex_7040_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-OPTI-050320/1144
<b>optiplex_7050_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-OPTI-050320/1145
<b>optiplex_7060_firmware</b>					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-OPTI-050320/1146
<b>optiplex_xe3_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-OPTI-050320/1147
<b>precision_3420_firmware</b>					
Missing	21-02-2020	2.1	Affected Dell Client	N/A	O-DEL-PREC-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication for Critical Function			platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		050320/1148
<b>precision_3430_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-PREC-050320/1149
<b>precision_3510_firmware</b>					
Missing Authentication	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS	N/A	O-DEL-PREC-050320/1150

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on for Critical Function			Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>precision_3520_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-PREC-050320/1151
<b>precision_3530_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File	N/A	O-DEL-PREC-050320/1152

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>		
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	O-DEL-PREC-050320/1153
<b>precision_3620_firmware</b>					
Missing Authentication for	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration	N/A	O-DEL-PREC-050320/1154

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Critical Function			authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>inspiron_3670_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-INSP-050320/1155
<b>inspiron_5488_firmware</b>					
Missing Authentication for Critical	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass	N/A	O-DEL-INSP-050320/1156

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Function			vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>optiplex_3070_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-OPTI-050320/1157
<b>optiplex_3240_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot	N/A	O-DEL-OPTI-050320/1158

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>optiplex_5070_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-OPTI-050320/1159
<b>optiplex_5250_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage	N/A	O-DEL-OPTI-050320/1160

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>optiplex_5260_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-OPTI-050320/1161
<b>optiplex_7070_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST)	N/A	O-DEL-OPTI-050320/1162

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>optiplex_7440_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-OPTI-050320/1163
<b>optiplex_7450_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker	N/A	O-DEL-OPTI-050320/1164

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>optiplex_7460_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-OPTI-050320/1165
<b>optiplex_7760_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the	N/A	O-DEL-OPTI-050320/1166

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>optiplex_5270_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-OPTI-050320/1167
<b>optiplex_7470_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform	N/A	O-DEL-OPTI-050320/1168

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>optiplex_7770_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-OPTI-050320/1169
<b>precision_5720_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the	N/A	O-DEL-PREC-050320/1170

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>precision_5810_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-PREC-050320/1171
<b>precision_7810_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration	N/A	O-DEL-PREC-050320/1172

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>precision_7910_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-PREC-050320/1173
<b>precision_3431_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring	N/A	O-DEL-PREC-050320/1174

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>vostro_15_7570_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-VOST-050320/1175
<b>xps_12_9250_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by	N/A	O-DEL-XPS_-050320/1176

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>xps_13_9343_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-XPS_-050320/1177
<b>xps_13_9350_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized	N/A	O-DEL-XPS_-050320/1178

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>xps_13_9360_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-XPS_-050320/1179
<b>xps_15_9550_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-	N/A	O-DEL-XPS_-050320/1180

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		
<b>xps_15_9560_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-XPS_-050320/1181
<b>xps_27_7760_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.	N/A	O-DEL-XPS_-050320/1182

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-5326</b>		
<b>inspiron_3470_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-INSP-050320/1183
<b>inspiron_3480_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility	N/A	O-DEL-INSP-050320/1184

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			delivers. <b>CVE ID : CVE-2020-5324</b>		
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-INSP-050320/1185
<b>inspiron_3481_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility	N/A	O-DEL-INSP-050320/1186

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			delivers. <b>CVE ID : CVE-2020-5324</b>		
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-INSP-050320/1187
<b>inspiron_3580_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility	N/A	O-DEL-INSP-050320/1188

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			delivers. <b>CVE ID : CVE-2020-5324</b>		
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-INSP-050320/1189
<b>inspiron_3583_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility	N/A	O-DEL-INSP-050320/1190

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			delivers. <b>CVE ID : CVE-2020-5324</b>		
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-INSP-050320/1191
<b>inspiron_3581_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility	N/A	O-DEL-INSP-050320/1192

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			delivers. <b>CVE ID : CVE-2020-5324</b>		
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-INSP-050320/1193
<b>inspiron_3584_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility	N/A	O-DEL-INSP-050320/1194

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			delivers. <b>CVE ID : CVE-2020-5324</b>		
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-INSP-050320/1195
<b>inspiron_3780_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility	N/A	O-DEL-INSP-050320/1196

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			delivers. <b>CVE ID : CVE-2020-5324</b>		
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-INSP-050320/1197
<b>inspiron_3781_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility	N/A	O-DEL-INSP-050320/1198

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			delivers. <b>CVE ID : CVE-2020-5324</b>		
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-INSP-050320/1199
<b>inspiron_5370_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-INSP-050320/1200

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<b>inspiron_5480_firmware</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	O-DEL-INSP-050320/1201
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	O-DEL-INSP-050320/1202

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<b>inspiron_5481_firmware</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	O-DEL-INSP-050320/1203
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	O-DEL-INSP-050320/1204

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<b>inspiron_5482_firmware</b>					
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	O-DEL-INSP-050320/1205
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	O-DEL-INSP-050320/1206

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<b>inspiron_5570_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.  <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-INSP-050320/1207
<b>inspiron_5580_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.	N/A	O-DEL-INSP-050320/1208

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-5324</b>		
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-INSP-050320/1209
<b>inspiron_5582_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.	N/A	O-DEL-INSP-050320/1210

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-5324</b>		
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-INSP-050320/1211
<b>inspiron_5770_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-INSP-050320/1212
<b>inspiron_7380_firmware</b>					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	O-DEL-INSP-050320/1213
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	O-DEL-INSP-050320/1214
inspiron_7386_firmware					

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	O-DEL-INSP-050320/1215
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	O-DEL-INSP-050320/1216
inspiron_7472_firmware					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-INSP-050320/1217
<b>inspiron_7580_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	O-DEL-INSP-050320/1218

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-INSP-050320/1219
<b>inspiron_7586_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	O-DEL-INSP-050320/1220

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-INSP-050320/1221
<b>inspiron_7786_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	O-DEL-INSP-050320/1222

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-INSP-050320/1223
<b>vostro_3470_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-VOST-050320/1224
<b>vostro_3480_firmware</b>					
Improper	21-02-2020	2.6	Dell Client Consumer and	N/A	O-DEL-VOST-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.  <b>CVE ID : CVE-2020-5324</b>		050320/1225
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.  <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-VOST-050320/1226
<b>vostro_3580_firmware</b>					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	O-DEL-VOST-050320/1227
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	O-DEL-VOST-050320/1228
<b>vostro_3581_firmware</b>					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	O-DEL-VOST-050320/1229
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	O-DEL-VOST-050320/1230
<b>vostro_3584_firmware</b>					

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	O-DEL-VOST-050320/1231
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	O-DEL-VOST-050320/1232
<b>vostro_3583_firmware</b>					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	21-02-2020	2.6	<p>Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers.</p> <p><b>CVE ID : CVE-2020-5324</b></p>	N/A	O-DEL-VOST-050320/1233
Missing Authentication for Critical Function	21-02-2020	2.1	<p>Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager.</p> <p><b>CVE ID : CVE-2020-5326</b></p>	N/A	O-DEL-VOST-050320/1234
<b>vostro_3670_firmware</b>					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-VOST-050320/1235
<b>vostro_5370_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-VOST-050320/1236
<b>vostro_5471_firmware</b>					
Missing	21-02-2020	2.1	Affected Dell Client	N/A	O-DEL-VOST-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication for Critical Function			platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		050320/1237
<b>vostro_5481_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	O-DEL-VOST-050320/1238

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-VOST-050320/1239
<b>vostro_5581_firmware</b>					
Improper Input Validation	21-02-2020	2.6	Dell Client Consumer and Commercial Platforms contain an Arbitrary File Overwrite Vulnerability. The vulnerability is limited to the Dell Firmware Update Utility during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. <b>CVE ID : CVE-2020-5324</b>	N/A	O-DEL-VOST-050320/1240

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-VOST-050320/1241
<b>wyse_5070_firmware</b>					
Missing Authentication for Critical Function	21-02-2020	2.1	Affected Dell Client platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>	N/A	O-DEL-WYSE-050320/1242
<b>wyse_7040_firmware</b>					
Missing	21-02-2020	2.1	Affected Dell Client	N/A	O-DEL-WYSE-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication for Critical Function			platforms contain a BIOS Setup configuration authentication bypass vulnerability in the pre-boot Intel Rapid Storage Response Technology (iRST) Manager menu. An attacker with physical access to the system could perform unauthorized changes to the BIOS Setup configuration settings without requiring the BIOS Admin password by selecting the Optimized Defaults option in the pre-boot iRST Manager. <b>CVE ID : CVE-2020-5326</b>		050320/1243

#### Dlink

#### dap-1330\_firmware

Improper Authentication	22-02-2020	8.3	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DAP-1330 1.10B01 BETA Wi-Fi range extenders. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of HNAP login requests. The issue results from the lack of proper handling of cookies. An attacker can leverage this vulnerability to execute arbitrary code on the router. Was ZDI-CAN-9554. <b>CVE ID : CVE-2020-8861</b>	N/A	O-DLI-DAP--050320/1244
-------------------------	------------	-----	--	-----	------------------------

#### dap-2610\_firmware

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	22-02-2020	8.3	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DAP-2610 Firmware v2.01RC067 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of passwords. The issue results from the lack of proper password checking. An attacker can leverage this vulnerability to execute arbitrary code in the context of root. Was ZDI-CAN-10082. <b>CVE ID : CVE-2020-8862</b>	N/A	O-DLI-DAP--050320/1245

#### D-link

#### dch-m225\_firmware

Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-02-2020	10	D-Link DCH-M225 1.05b01 and earlier devices allow remote attackers to execute arbitrary OS commands via shell metacharacters in the spotifyConnect.php userName parameter. <b>CVE ID : CVE-2020-6841</b>	<a href="https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10152">https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10152</a>	O-D-L-DCH--050320/1246
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-02-2020	9	D-Link DCH-M225 1.05b01 and earlier devices allow remote authenticated admins to execute arbitrary OS commands via shell metacharacters in the media renderer name. <b>CVE ID : CVE-2020-6842</b>	<a href="https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10152">https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10152</a>	O-D-L-DCH--050320/1247

#### eltex-co

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<b>ntp-2_firmware</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-02-2020	10	ELTEX NTP-RG-1402G 1v10 3.25.3.32 devices allow OS command injection via the PING field of the resource ping.cmd. The NTP-2 device is also affected. <b>CVE ID : CVE-2020-9026</b>	N/A	O-ELT-NTP--050320/1248
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-02-2020	10	ELTEX NTP-RG-1402G 1v10 3.25.3.32 devices allow OS command injection via the TRACE field of the resource ping.cmd. The NTP-2 device is also affected. <b>CVE ID : CVE-2020-9027</b>	N/A	O-ELT-NTP--050320/1249
<b>ntp-rg-1402g_firmware</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-02-2020	10	ELTEX NTP-RG-1402G 1v10 3.25.3.32 devices allow OS command injection via the PING field of the resource ping.cmd. The NTP-2 device is also affected. <b>CVE ID : CVE-2020-9026</b>	N/A	O-ELT-NTP--050320/1250
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-02-2020	10	ELTEX NTP-RG-1402G 1v10 3.25.3.32 devices allow OS command injection via the TRACE field of the resource ping.cmd. The NTP-2 device is also affected. <b>CVE ID : CVE-2020-9027</b>	N/A	O-ELT-NTP--050320/1251
<b>Fedoraproject</b>					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
<b>fedora</b>					
Improper Control of Generation of Code ('Code Injection')	17-02-2020	7.5	Horde Groupware Webmail Edition 5.2.22 allows injection of arbitrary PHP code via CSV data, leading to remote code execution. <b>CVE ID : CVE-2020-8518</b>	<a href="https://lists.horde.org/archives/announce/2020/001285.html">https://lists.horde.org/archives/announce/2020/001285.html</a>	O-FED-FEDO-050320/1252
<b>hitrontech</b>					
<b>coda-4582u_firmware</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-02-2020	3.5	Hitron CODA-4582U 7.1.1.30 devices allow XSS via a Managed Device name on the Wireless > Access Control > Add Managed Device screen. <b>CVE ID : CVE-2020-8824</b>	N/A	O-HIT-CODA-050320/1253
<b>Honeywell</b>					
<b>inncom_inncontrol_firmware</b>					
Improper Privilege Management	20-02-2020	4.6	Honeywell INNCOM INNControl 3 allows workstation users to escalate application user privileges through the modification of local configuration files. <b>CVE ID : CVE-2020-6968</b>	N/A	O-HON-INNC-050320/1254
<b>Huawei</b>					
<b>honor_magic2_firmware</b>					
Incorrect Authorization	18-02-2020	2.1	Huawei mobile phones Ever-L29B versions earlier than 10.0.0.180(C185E6R3P3), earlier than 10.0.0.180(C432E6R1P7), earlier than 10.0.0.180(C636E5R2P3); HUAWEI Mate 20 RS	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-phone-">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-phone-</a>	O-HUA-HONO-050320/1255

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions earlier than 10.0.0.175(C786E70R3P8); HUAWEI Mate 20 X versions earlier than 10.0.0.176(C00E70R2P8); and Honor Magic2 versions earlier than 10.0.0.175(C00E59R2P11) have an improper authorization vulnerability. Due to improper authorization of some function, attackers can bypass the authorization to perform some operations. <b>CVE ID : CVE-2020-1882</b>	en	
<b>nip6300_firmware</b>					
Information Exposure	17-02-2020	5	Huawei NGFW Module, NIP6300, NIP6600, Secospace USG6500, Secospace USG6600, and USG9500 versions V500R001C30, V500R001C60, and V500R005C00 have an information leakage vulnerability. An attacker can exploit this vulnerability by sending specific request packets to affected devices. Successful exploit may lead to information leakage. <b>CVE ID : CVE-2020-1856</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-firewall-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-firewall-en</a>	O-HUA-NIP6-050320/1256
<b>nip6600_firmware</b>					
Information Exposure	17-02-2020	5	Huawei NGFW Module, NIP6300, NIP6600, Secospace USG6500, Secospace USG6600, and USG9500 versions	<a href="http://www.huawei.com/en/psirt/security-advisories/">http://www.huawei.com/en/psirt/security-advisories/</a>	O-HUA-NIP6-050320/1257

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R001C30, V500R001C60, and V500R005C00 have an information leakage vulnerability. An attacker can exploit this vulnerability by sending specific request packets to affected devices. Successful exploit may lead to information leakage. <b>CVE ID : CVE-2020-1856</b>	huawei-sa-20200205-01-firewall-en	
<b>nip6800_firmware</b>					
NULL Pointer Dereference	18-02-2020	3.5	Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00; Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00 have a Dangling pointer dereference vulnerability. An authenticated attacker may do some special operations in the affected products in some special scenarios to exploit the vulnerability. Due to improper race conditions of different operations, successful exploit will lead to Dangling pointer dereference, causing some service abnormal. <b>CVE ID : CVE-2020-1814</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-01-firewall-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-01-firewall-en</a>	O-HUA-NIP6-050320/1258
Missing Release of Resource	18-02-2020	4.3	Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and	<a href="http://www.huawei.com/en/psirt">http://www.huawei.com/en/psirt</a>	O-HUA-NIP6-050320/1259

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
after Effective Lifetime			V500R005C00; Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00 have a memory leak vulnerability. The software does not sufficiently track and release allocated memory while parse certain message, the attacker sends the message continuously that could consume remaining memory. Successful exploit could cause memory exhaust.  <b>CVE ID : CVE-2020-1815</b>	t/security- advisories/ huawei-sa- 20200212- 02-firewall- en	
Improper Input Validation	18-02-2020	4.3	Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00; Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00 have a Denial of Service (DoS) vulnerability. Due to improper processing of specific IPSEC packets, remote attackers can send constructed IPSEC packets to affected devices to exploit this vulnerability. Successful exploit could cause the IPSec function of the affected device abnormal.	http://ww w.huawei.c om/en/psir t/security- advisories/ huawei-sa- 20200212- 03-firewall- en	O-HUA-NIP6- 050320/1260

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-1816</b>		
Improper Resource Shutdown or Release	17-02-2020	5	<p>Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00SPC100; and Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00SPC100 have an information leakage vulnerability. An attacker can exploit this vulnerability by sending specific request packets to affected devices. Successful exploit may lead to information leakage.</p> <p><b>CVE ID : CVE-2020-1827</b></p>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-02-ipsec-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-02-ipsec-en</a>	O-HUA-NIP6-050320/1261
Improper Input Validation	17-02-2020	5	<p>Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00; and Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00 have an input validation vulnerability where the IPSec module does not validate a field in a specific message. Attackers can send specific message to cause out-of-bound read, compromising normal service.</p> <p><b>CVE ID : CVE-2020-1828</b></p>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-01-ipsec-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-01-ipsec-en</a>	O-HUA-NIP6-050320/1262
Double Free	17-02-2020	5	Huawei NIP6800 versions V500R001C30 and	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-01-ipsec-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-01-ipsec-en</a>	O-HUA-NIP6-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R001C60SPC500; and Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, and V500R001C60SPC500 have a vulnerability that the IPSec module handles a message improperly. Attackers can send specific message to cause double free memory. This may compromise normal service. <b>CVE ID : CVE-2020-1829</b>	om/en/psirt/security-advisories/huawei-sa-20200212-03-ipsec-en	050320/1263
Out-of-bounds Read	18-02-2020	5	Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00; Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00 have a vulnerability that a memory management error exists when IPSec Module handing a specific message. This causes 1 byte out-of-bound read, compromising normal service. <b>CVE ID : CVE-2020-1830</b>	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-04-ipsec-en	O-HUA-NIP6-050320/1264
Information Exposure	17-02-2020	2.1	Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00SPC100; and Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600,	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-leakage-	O-HUA-NIP6-050320/1265

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R001C60SPC500, and V500R005C00SPC100 have an information leakage vulnerability. Due to improper processing of some data, a local authenticated attacker can exploit this vulnerability through a series of operations. Successful exploitation may cause information leakage. <b>CVE ID : CVE-2020-1857</b>	en	
N/A	17-02-2020	5	Huawei products NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00SPC100; Secospace USG6600 versions V500R001C30SPC600, V500R001C60SPC500, and V500R005C00SPC100; and USG9500 versions V500R001C30SPC600, V500R001C60SPC500, and V500R005C00SPC100 have a denial of service vulnerability. Attackers need to perform a series of operations in a special scenario to exploit this vulnerability. Successful exploit may cause the new connections can't be established, result in a denial of service. <b>CVE ID : CVE-2020-1858</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-dos-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-dos-en</a> , <a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200219-04-dos-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200219-04-dos-en</a>	O-HUA-NIP6-050320/1266
Access of Uninitialized Pointer	28-02-2020	4.9	NIP6800;Secospace USG6600;USG9500 products versions of V500R001C30; V500R001C60SPC500;	N/A	O-HUA-NIP6-050320/1267

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R005C00SPC100 have a invalid pointer access vulnerability. The software system access an invalid pointer when operator logs in to the device and performs some operations. Successful exploit could cause certain process reboot. <b>CVE ID : CVE-2020-1874</b>		
Access of Uninitialized Pointer	28-02-2020	4.9	NIP6800;Secospace USG6600;USG9500 with versions of V500R001C30; V500R001C60SPC500; V500R005C00SPC100 have an invalid pointer access vulnerability. The software system access an invalid pointer when administrator log in to the device and performs some operations. Successful exploit could cause certain process reboot. <b>CVE ID : CVE-2020-1877</b>	N/A	O-HUA-NIP6-050320/1268
Uncontrolled Resource Consumption	28-02-2020	5	NIP6800;Secospace USG6600;USG9500 products with versions of V500R001C30; V500R001C60SPC500; V500R005C00SPC100 have have a resource management error vulnerability. An attacker needs to perform specific operations to trigger a function of the affected device. Due to improper resource management of the function, the vulnerability can be exploited to cause	N/A	O-HUA-NIP6-050320/1269

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service abnormal on affected devices. <b>CVE ID : CVE-2020-1881</b>		
<b>secospace_usg6500_firmware</b>					
Information Exposure	17-02-2020	5	Huawei NGFW Module, NIP6300, NIP6600, Secospace USG6500, Secospace USG6600, and USG9500 versions V500R001C30, V500R001C60, and V500R005C00 have an information leakage vulnerability. An attacker can exploit this vulnerability by sending specific request packets to affected devices. Successful exploit may lead to information leakage. <b>CVE ID : CVE-2020-1856</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-firewall-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-firewall-en</a>	O-HUA-SECO-050320/1270
<b>secospace_usg6600_firmware</b>					
NULL Pointer Dereference	18-02-2020	3.5	Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00; Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00 have a Dangling pointer dereference vulnerability. An authenticated attacker may do some special operations in the affected products in some special scenarios to exploit the vulnerability. Due to	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-01-firewall-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-01-firewall-en</a>	O-HUA-SECO-050320/1271

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improper race conditions of different operations, successful exploit will lead to Dangling pointer dereference, causing some service abnormal. <b>CVE ID : CVE-2020-1814</b>		
Missing Release of Resource after Effective Lifetime	18-02-2020	4.3	Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00; Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00 have a memory leak vulnerability. The software does not sufficiently track and release allocated memory while parse certain message, the attacker sends the message continuously that could consume remaining memory. Successful exploit could cause memory exhaust. <b>CVE ID : CVE-2020-1815</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-02-firewall-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-02-firewall-en</a>	O-HUA-SECO-050320/1272
Improper Input Validation	18-02-2020	4.3	Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00; Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00 have a Denial of Service (DoS)	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-03-firewall-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-03-firewall-en</a>	O-HUA-SECO-050320/1273

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. Due to improper processing of specific IPSEC packets, remote attackers can send constructed IPSEC packets to affected devices to exploit this vulnerability. Successful exploit could cause the IPSec function of the affected device abnormal. <b>CVE ID : CVE-2020-1816</b>		
Improper Resource Shutdown or Release	17-02-2020	5	Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00SPC100; and Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00SPC100 have an information leakage vulnerability. An attacker can exploit this vulnerability by sending specific request packets to affected devices. Successful exploit may lead to information leakage. <b>CVE ID : CVE-2020-1827</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-02-ipsec-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-02-ipsec-en</a>	O-HUA-SECO-050320/1274
Improper Input Validation	17-02-2020	5	Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00; and Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00 have an input validation vulnerability	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-01-ipsec-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-01-ipsec-en</a>	O-HUA-SECO-050320/1275

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			where the IPSec module does not validate a field in a specific message. Attackers can send specific message to cause out-of-bound read, compromising normal service. <b>CVE ID : CVE-2020-1828</b>		
Double Free	17-02-2020	5	Huawei NIP6800 versions V500R001C30 and V500R001C60SPC500; and Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, and V500R001C60SPC500 have a vulnerability that the IPSec module handles a message improperly. Attackers can send specific message to cause double free memory. This may compromise normal service. <b>CVE ID : CVE-2020-1829</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-03-ipsec-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-03-ipsec-en</a>	O-HUA-SECO-050320/1276
Out-of-bounds Read	18-02-2020	5	Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00; Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00 have a vulnerability that a memory management error exists when IPSec Module handing a specific message. This causes 1 byte out-of-bound read, compromising normal	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-04-ipsec-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-04-ipsec-en</a>	O-HUA-SECO-050320/1277

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service. <b>CVE ID : CVE-2020-1830</b>		
Information Exposure	17-02-2020	5	Huawei NGFW Module, NIP6300, NIP6600, Secospace USG6500, Secospace USG6600, and USG9500 versions V500R001C30, V500R001C60, and V500R005C00 have an information leakage vulnerability. An attacker can exploit this vulnerability by sending specific request packets to affected devices. Successful exploit may lead to information leakage. <b>CVE ID : CVE-2020-1856</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-firewall-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-firewall-en</a>	O-HUA-SECO-050320/1278
Information Exposure	17-02-2020	2.1	Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00SPC100; and Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00SPC100 have an information leakage vulnerability. Due to improper processing of some data, a local authenticated attacker can exploit this vulnerability through a series of operations. Successful exploitation may cause information leakage. <b>CVE ID : CVE-2020-1857</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-leakage-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-leakage-en</a>	O-HUA-SECO-050320/1279

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	17-02-2020	5	<p>Huawei products NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00SPC100; Secospace USG6600 versions V500R001C30SPC600, V500R001C60SPC500, and V500R005C00SPC100; and USG9500 versions V500R001C30SPC600, V500R001C60SPC500, and V500R005C00SPC100 have a denial of service vulnerability. Attackers need to perform a series of operations in a special scenario to exploit this vulnerability. Successful exploit may cause the new connections can't be established, result in a denial of service.</p> <p><b>CVE ID : CVE-2020-1858</b></p>	<p><a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-dos-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-dos-en</a>, <a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200219-04-dos-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200219-04-dos-en</a></p>	O-HUA-SECO-050320/1280
Access of Uninitialized Pointer	28-02-2020	4.9	<p>NIP6800;Secospace USG6600;USG9500 products versions of V500R001C30; V500R001C60SPC500; V500R005C00SPC100 have a invalid pointer access vulnerability. The software system access an invalid pointer when operator logs in to the device and performs some operations. Successful exploit could cause certain process reboot.</p> <p><b>CVE ID : CVE-2020-1874</b></p>	N/A	O-HUA-SECO-050320/1281
Access of Uninitialized Pointer	28-02-2020	4.9	<p>NIP6800;Secospace USG6600;USG9500 with versions of V500R001C30;</p>	N/A	O-HUA-SECO-050320/1282

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R001C60SPC500; V500R005C00SPC100 have an invalid pointer access vulnerability. The software system access an invalid pointer when administrator log in to the device and performs some operations. Successful exploit could cause certain process reboot. <b>CVE ID : CVE-2020-1877</b>		
Uncontrolled Resource Consumption	28-02-2020	5	NIP6800;Secospace USG6600;USG9500 products with versions of V500R001C30; V500R001C60SPC500; V500R005C00SPC100 have a resource management error vulnerability. An attacker needs to perform specific operations to trigger a function of the affected device. Due to improper resource management of the function, the vulnerability can be exploited to cause service abnormal on affected devices. <b>CVE ID : CVE-2020-1881</b>	N/A	O-HUA-SECO-050320/1283
<b>p30_firmware</b>					
Improper Authentication	18-02-2020	6.8	HUAWEI P30 smartphones with versions earlier than 10.0.0.173(C00E73R1P11) have an improper authentication vulnerability. Due to improperly validation of certain application, an attacker should trick the user into installing a	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200120-01-smartphone">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200120-01-smartphone</a>	O-HUA-P30_-050320/1284

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious application to exploit this vulnerability. Successful exploit could allow the attacker to bypass the authentication to perform unauthorized operations. <b>CVE ID : CVE-2020-1812</b>	-en	
<b>mate_20_x_firmware</b>					
Incorrect Authorization	18-02-2020	2.1	Huawei mobile phones Ever-L29B versions earlier than 10.0.0.180(C185E6R3P3), earlier than 10.0.0.180(C432E6R1P7), earlier than 10.0.0.180(C636E5R2P3); HUAWEI Mate 20 RS versions earlier than 10.0.0.175(C786E70R3P8); HUAWEI Mate 20 X versions earlier than 10.0.0.176(C00E70R2P8); and Honor Magic2 versions earlier than 10.0.0.175(C00E59R2P11) have an improper authorization vulnerability. Due to improper authorization of some function, attackers can bypass the authorization to perform some operations. <b>CVE ID : CVE-2020-1882</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-phone-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-phone-en</a>	O-HUA-MATE-050320/1285
<b>mate_20_firmware</b>					
Incorrect Authorization	18-02-2020	2.1	HUAWEI Mate 20 smartphones with versions earlier than 10.0.0.185(C00E74R3P8) have an improper	<a href="http://www.huawei.com/en/psirt/security-advisories/">http://www.huawei.com/en/psirt/security-advisories/</a>	O-HUA-MATE-050320/1286

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authorization vulnerability. The system has a logic judging error under certain scenario, successful exploit could allow the attacker to switch to third desktop after a series of operation in ADB mode. <b>CVE ID : CVE-2020-1791</b>	huawei-sa-20200205-01-smartphone-en	
<b>osca-550_firmware</b>					
Improper Authentication	18-02-2020	4.6	Huawei OSCA-550, OSCA-550A, OSCA-550AX, and OSCA-550X products with version 1.0.1.21(SP3) have an insufficient authentication vulnerability. The software does not require a strong credential when the user trying to do certain operations. Successful exploit could allow an attacker to pass the authentication and do certain operations by a weak credential. <b>CVE ID : CVE-2020-1789</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200121-01-osca-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200121-01-osca-en</a>	O-HUA-OSCA-050320/1287
Improper Authentication	18-02-2020	4.6	Huawei HEGE-560 version 1.0.1.20(SP2); OSCA-550 and OSCA-550A version 1.0.0.71(SP1); and OSCA-550AX and OSCA-550X version 1.0.0.71(SP2) have an insufficient authentication vulnerability. An attacker can access the device physically and perform specific operations to exploit this vulnerability. Successful exploitation may cause the attacker obtain	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-osca-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-osca-en</a>	O-HUA-OSCA-050320/1288

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			high privilege. <b>CVE ID : CVE-2020-1842</b>		
Improper Input Validation	18-02-2020	4.6	Huawei HEGE-560 version 1.0.1.20(SP2), OSCA-550 version 1.0.0.71(SP1), OSCA-550A version 1.0.0.71(SP1), OSCA-550AX version 1.0.0.71(SP2), and OSCA-550X version 1.0.0.71(SP2) have an insufficient verification vulnerability. An attacker can perform specific operations to exploit this vulnerability by physical access methods. Successful exploitation may cause the attacker perform an illegal operation. <b>CVE ID : CVE-2020-1843</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-02-osca-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-02-osca-en</a>	O-HUA-OSCA-050320/1289
Improper Input Validation	18-02-2020	3.6	Huawei HEGE-570 version 1.0.1.22(SP3); and HEGE-560, OSCA-550, OSCA-550A, OSCA-550AX, and OSCA-550X version 1.0.1.21(SP3) have an insufficient verification vulnerability. An attacker can access the device physically and exploit this vulnerability to tamper with device information. Successful exploit may cause service abnormal. <b>CVE ID : CVE-2020-1855</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-03-osca-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-03-osca-en</a>	O-HUA-OSCA-050320/1290
<b>osca-550a_firmware</b>					
Improper Authentication	18-02-2020	4.6	Huawei OSCA-550, OSCA-550A, OSCA-550AX, and OSCA-550X products with version 1.0.1.21(SP3) have an insufficient	<a href="http://www.huawei.com/en/psirt/security-advisories/">http://www.huawei.com/en/psirt/security-advisories/</a>	O-HUA-OSCA-050320/1291

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authentication vulnerability. The software does not require a strong credential when the user trying to do certain operations. Successful exploit could allow an attacker to pass the authentication and do certain operations by a weak credential. <b>CVE ID : CVE-2020-1789</b>	huawei-sa-20200121-01-osca-en	
Improper Authentication	18-02-2020	4.6	Huawei HEGE-560 version 1.0.1.20(SP2); OSCA-550 and OSCA-550A version 1.0.0.71(SP1); and OSCA-550AX and OSCA-550X version 1.0.0.71(SP2) have an insufficient authentication vulnerability. An attacker can access the device physically and perform specific operations to exploit this vulnerability. Successful exploitation may cause the attacker obtain high privilege. <b>CVE ID : CVE-2020-1842</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-osca-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-osca-en</a>	O-HUA-OSCA-050320/1292
Improper Input Validation	18-02-2020	4.6	Huawei HEGE-560 version 1.0.1.20(SP2), OSCA-550 version 1.0.0.71(SP1), OSCA-550A version 1.0.0.71(SP1), OSCA-550AX version 1.0.0.71(SP2), and OSCA-550X version 1.0.0.71(SP2) have an insufficient verification vulnerability. An attacker can perform specific operations to exploit this vulnerability by physical access methods. Successful	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-02-osca-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-02-osca-en</a>	O-HUA-OSCA-050320/1293

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation may cause the attacker perform an illegal operation. <b>CVE ID : CVE-2020-1843</b>		
Improper Input Validation	18-02-2020	3.6	Huawei HEGE-570 version 1.0.1.22(SP3); and HEGE-560, OSCA-550, OSCA-550A, OSCA-550AX, and OSCA-550X version 1.0.1.21(SP3) have an insufficient verification vulnerability. An attacker can access the device physically and exploit this vulnerability to tamper with device information. Successful exploit may cause service abnormal. <b>CVE ID : CVE-2020-1855</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-03-osca-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-03-osca-en</a>	O-HUA-OSCA-050320/1294
<b>osca-550ax_firmware</b>					
Improper Authentication	18-02-2020	4.6	Huawei OSCA-550, OSCA-550A, OSCA-550AX, and OSCA-550X products with version 1.0.1.21(SP3) have an insufficient authentication vulnerability. The software does not require a strong credential when the user trying to do certain operations. Successful exploit could allow an attacker to pass the authentication and do certain operations by a weak credential. <b>CVE ID : CVE-2020-1789</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200121-01-osca-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200121-01-osca-en</a>	O-HUA-OSCA-050320/1295
Improper Authentication	18-02-2020	4.6	Huawei HEGE-560 version 1.0.1.20(SP2); OSCA-550 and OSCA-550A version 1.0.0.71(SP1); and OSCA-	<a href="http://www.huawei.com/en/psirt/security-">http://www.huawei.com/en/psirt/security-</a>	O-HUA-OSCA-050320/1296

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			550AX and OSCA-550X version 1.0.0.71(SP2) have an insufficient authentication vulnerability. An attacker can access the device physically and perform specific operations to exploit this vulnerability. Successful exploitation may cause the attacker obtain high privilege. <b>CVE ID : CVE-2020-1842</b>	advisories/huawei-sa-20200122-01-osca-en	
Improper Input Validation	18-02-2020	4.6	Huawei HEGE-560 version 1.0.1.20(SP2), OSCA-550 version 1.0.0.71(SP1), OSCA-550A version 1.0.0.71(SP1), OSCA-550AX version 1.0.0.71(SP2), and OSCA-550X version 1.0.0.71(SP2) have an insufficient verification vulnerability. An attacker can perform specific operations to exploit this vulnerability by physical access methods. Successful exploitation may cause the attacker perform an illegal operation. <b>CVE ID : CVE-2020-1843</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-02-osca-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-02-osca-en</a>	O-HUA-OSCA-050320/1297
Improper Input Validation	18-02-2020	3.6	Huawei HEGE-570 version 1.0.1.22(SP3); and HEGE-560, OSCA-550, OSCA-550A, OSCA-550AX, and OSCA-550X version 1.0.1.21(SP3) have an insufficient verification vulnerability. An attacker can access the device physically and exploit this vulnerability to tamper with device information.	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-03-osca-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-03-osca-en</a>	O-HUA-OSCA-050320/1298

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful exploit may cause service abnormal. <b>CVE ID : CVE-2020-1855</b>		
<b>osca-550x_firmware</b>					
Improper Authentication	18-02-2020	4.6	Huawei OSCA-550, OSCA-550A, OSCA-550AX, and OSCA-550X products with version 1.0.1.21(SP3) have an insufficient authentication vulnerability. The software does not require a strong credential when the user trying to do certain operations. Successful exploit could allow an attacker to pass the authentication and do certain operations by a weak credential. <b>CVE ID : CVE-2020-1789</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200121-01-osca-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200121-01-osca-en</a>	O-HUA-OSCA-050320/1299
Improper Authentication	18-02-2020	4.6	Huawei HEGE-560 version 1.0.1.20(SP2); OSCA-550 and OSCA-550A version 1.0.0.71(SP1); and OSCA-550AX and OSCA-550X version 1.0.0.71(SP2) have an insufficient authentication vulnerability. An attacker can access the device physically and perform specific operations to exploit this vulnerability. Successful exploitation may cause the attacker obtain high privilege. <b>CVE ID : CVE-2020-1842</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-osca-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-osca-en</a>	O-HUA-OSCA-050320/1300
Improper Input Validation	18-02-2020	4.6	Huawei HEGE-560 version 1.0.1.20(SP2), OSCA-550 version 1.0.0.71(SP1), OSCA-	<a href="http://www.huawei.com/en/psirt">http://www.huawei.com/en/psirt</a>	O-HUA-OSCA-050320/1301

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			550A version 1.0.0.71(SP1), OSCA-550AX version 1.0.0.71(SP2), and OSCA-550X version 1.0.0.71(SP2) have an insufficient verification vulnerability. An attacker can perform specific operations to exploit this vulnerability by physical access methods. Successful exploitation may cause the attacker perform an illegal operation. <b>CVE ID : CVE-2020-1843</b>	t/security-advisories/huawei-sa-20200122-02-osca-en	
Improper Input Validation	18-02-2020	3.6	Huawei HEGE-570 version 1.0.1.22(SP3); and HEGE-560, OSCA-550, OSCA-550A, OSCA-550AX, and OSCA-550X version 1.0.1.21(SP3) have an insufficient verification vulnerability. An attacker can access the device physically and exploit this vulnerability to tamper with device information. Successful exploit may cause service abnormal. <b>CVE ID : CVE-2020-1855</b>	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-03-osca-en	O-HUA-OSCA-050320/1302
<b>cloudlink_board_firmware</b>					
Information Exposure	17-02-2020	5	Huawei CloudLink Board version 20.0.0; DP300 version V500R002C00; RSE6500 versions V100R001C00, V500R002C00, and V500R002C00SPC900; and TE60 versions V500R002C00, V600R006C00, V600R006C00SPC200,	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200207-01-te-en	O-HUA-CLOU-050320/1303

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V600R006C00SPC300, V600R006C10, V600R019C00, and V600R019C00SPC100 have an information leak vulnerability. An unauthenticated, remote attacker can make a large number of attempts to guess information. Successful exploitation may cause information leak. <b>CVE ID : CVE-2020-1841</b>		
<b>dp300_firmware</b>					
Information Exposure	17-02-2020	5	Huawei CloudLink Board version 20.0.0; DP300 version V500R002C00; RSE6500 versions V100R001C00, V500R002C00, and V500R002C00SPC900; and TE60 versions V500R002C00, V600R006C00, V600R006C00SPC200, V600R006C00SPC300, V600R006C10, V600R019C00, and V600R019C00SPC100 have an information leak vulnerability. An unauthenticated, remote attacker can make a large number of attempts to guess information. Successful exploitation may cause information leak. <b>CVE ID : CVE-2020-1841</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200207-01-te-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200207-01-te-en</a>	O-HUA-DP30-050320/1304
<b>rse6500_firmware</b>					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	17-02-2020	5	<p>Huawei CloudLink Board version 20.0.0; DP300 version V500R002C00; RSE6500 versions V100R001C00, V500R002C00, and V500R002C00SPC900; and TE60 versions V500R002C00, V600R006C00, V600R006C00SPC200, V600R006C00SPC300, V600R006C10, V600R019C00, and V600R019C00SPC100 have an information leak vulnerability. An unauthenticated, remote attacker can make a large number of attempts to guess information. Successful exploitation may cause information leak.</p> <p><b>CVE ID : CVE-2020-1841</b></p>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200207-01-te-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200207-01-te-en</a>	O-HUA-RSE6-050320/1305
<b>te60_firmware</b>					
Information Exposure	17-02-2020	5	<p>Huawei CloudLink Board version 20.0.0; DP300 version V500R002C00; RSE6500 versions V100R001C00, V500R002C00, and V500R002C00SPC900; and TE60 versions V500R002C00, V600R006C00, V600R006C00SPC200, V600R006C00SPC300, V600R006C10, V600R019C00, and V600R019C00SPC100 have</p>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200207-01-te-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200207-01-te-en</a>	O-HUA-TE60-050320/1306

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an information leak vulnerability. An unauthenticated, remote attacker can make a large number of attempts to guess information. Successful exploitation may cause information leak. <b>CVE ID : CVE-2020-1841</b>		
<b>hege-560_firmware</b>					
Improper Authentication	18-02-2020	4.6	Huawei HEGE-560 version 1.0.1.20(SP2); OSCA-550 and OSCA-550A version 1.0.0.71(SP1); and OSCA-550AX and OSCA-550X version 1.0.0.71(SP2) have an insufficient authentication vulnerability. An attacker can access the device physically and perform specific operations to exploit this vulnerability. Successful exploitation may cause the attacker obtain high privilege. <b>CVE ID : CVE-2020-1842</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-osca-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-osca-en</a>	O-HUA-HEGE-050320/1307
Improper Input Validation	18-02-2020	4.6	Huawei HEGE-560 version 1.0.1.20(SP2), OSCA-550 version 1.0.0.71(SP1), OSCA-550A version 1.0.0.71(SP1), OSCA-550AX version 1.0.0.71(SP2), and OSCA-550X version 1.0.0.71(SP2) have an insufficient verification vulnerability. An attacker can perform specific operations to exploit this vulnerability by physical access methods. Successful exploitation may cause the	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-02-osca-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-02-osca-en</a>	O-HUA-HEGE-050320/1308

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker perform an illegal operation. <b>CVE ID : CVE-2020-1843</b>		
Improper Input Validation	18-02-2020	3.6	Huawei HEGE-570 version 1.0.1.22(SP3); and HEGE-560, OSCA-550, OSCA-550A, OSCA-550AX, and OSCA-550X version 1.0.1.21(SP3) have an insufficient verification vulnerability. An attacker can access the device physically and exploit this vulnerability to tamper with device information. Successful exploit may cause service abnormal. <b>CVE ID : CVE-2020-1855</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-03-osca-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-03-osca-en</a>	O-HUA-HEGE-050320/1309
<b>hege-570_firmware</b>					
Improper Input Validation	18-02-2020	3.6	Huawei HEGE-570 version 1.0.1.22(SP3); and HEGE-560, OSCA-550, OSCA-550A, OSCA-550AX, and OSCA-550X version 1.0.1.21(SP3) have an insufficient verification vulnerability. An attacker can access the device physically and exploit this vulnerability to tamper with device information. Successful exploit may cause service abnormal. <b>CVE ID : CVE-2020-1855</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-03-osca-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-03-osca-en</a>	O-HUA-HEGE-050320/1310
<b>ngfw_module_firmware</b>					
Information Exposure	17-02-2020	5	Huawei NGFW Module, NIP6300, NIP6600, Secospace USG6500, Secospace USG6600, and USG9500 versions V500R001C30,	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-03-osca-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-</a>	O-HUA-NGFW-050320/1311

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R001C60, and V500R005C00 have an information leakage vulnerability. An attacker can exploit this vulnerability by sending specific request packets to affected devices. Successful exploit may lead to information leakage. <b>CVE ID : CVE-2020-1856</b>	20200205-01-firewall-en	
<b>p10_plus_firmware</b>					
Improper Input Validation	18-02-2020	2.1	Huawei smart phones P10 Plus with versions earlier than 9.1.0.201(C01E75R1P12T8), earlier than 9.1.0.252(C185E2R1P9T8), earlier than 9.1.0.252(C432E4R1P9T8), and earlier than 9.1.0.255(C576E6R1P8T8) have a digital balance bypass vulnerability. When re-configuring the mobile phone at the digital balance mode, an attacker can perform some operations to bypass the startup wizard, and then open some switch. As a result, the digital balance function is bypassed. <b>CVE ID : CVE-2020-1872</b>	<a href="https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-digitalbalance-en">https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-digitalbalance-en</a>	O-HUA-P10_-050320/1312
<b>mate_20_rs_firmware</b>					
Incorrect Authorization	18-02-2020	2.1	Huawei mobile phones Ever-L29B versions earlier than 10.0.0.180(C185E6R3P3), earlier than 10.0.0.180(C432E6R1P7), earlier than	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-</a>	O-HUA-MATE-050320/1313

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>10.0.0.180(C636E5R2P3); HUAWEI Mate 20 RS versions earlier than 10.0.0.175(C786E70R3P8); HUAWEI Mate 20 X versions earlier than 10.0.0.176(C00E70R2P8); and Honor Magic2 versions earlier than 10.0.0.175(C00E59R2P11) have an improper authorization vulnerability. Due to improper authorization of some function, attackers can bypass the authorization to perform some operations.</p> <p><b>CVE ID : CVE-2020-1882</b></p>	20200122-01-phone-en	
<b>ever-l29b_firmware</b>					
Incorrect Authorization	18-02-2020	2.1	<p>Huawei mobile phones Ever-L29B versions earlier than 10.0.0.180(C185E6R3P3), earlier than 10.0.0.180(C432E6R1P7), earlier than 10.0.0.180(C636E5R2P3); HUAWEI Mate 20 RS versions earlier than 10.0.0.175(C786E70R3P8); HUAWEI Mate 20 X versions earlier than 10.0.0.176(C00E70R2P8); and Honor Magic2 versions earlier than 10.0.0.175(C00E59R2P11) have an improper authorization vulnerability. Due to improper authorization of some function, attackers can</p>	<p><a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-phone-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200122-01-phone-en</a></p>	O-HUA-EVER-050320/1314

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			bypass the authorization to perform some operations. <b>CVE ID : CVE-2020-1882</b>		
<b>usg9500_firmware</b>					
NULL Pointer Dereference	18-02-2020	3.5	Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00; Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00 have a Dangling pointer dereference vulnerability. An authenticated attacker may do some special operations in the affected products in some special scenarios to exploit the vulnerability. Due to improper race conditions of different operations, successful exploit will lead to Dangling pointer dereference, causing some service abnormal. <b>CVE ID : CVE-2020-1814</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-01-firewall-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-01-firewall-en</a>	O-HUA-USG9-050320/1315
Missing Release of Resource after Effective Lifetime	18-02-2020	4.3	Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00; Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00 have a memory leak vulnerability.	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-02-firewall-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-02-firewall-en</a>	O-HUA-USG9-050320/1316

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>The software does not sufficiently track and release allocated memory while parse certain message, the attacker sends the message continuously that could consume remaining memory. Successful exploit could cause memory exhaust.</p> <p><b>CVE ID : CVE-2020-1815</b></p>		
Improper Input Validation	18-02-2020	4.3	<p>Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00; Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00 have a Denial of Service (DoS) vulnerability. Due to improper processing of specific IPSEC packets, remote attackers can send constructed IPSEC packets to affected devices to exploit this vulnerability. Successful exploit could cause the IPSec function of the affected device abnormal.</p> <p><b>CVE ID : CVE-2020-1816</b></p>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-03-firewall-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-03-firewall-en</a>	O-HUA-USG9-050320/1317
Improper Resource Shutdown or Release	17-02-2020	5	<p>Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00SPC100; and Secospace USG6600 and USG9500 versions V500R001C30SPC200,</p>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-</a>	O-HUA-USG9-050320/1318

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R001C30SPC600, V500R001C60SPC500, and V500R005C00SPC100 have an information leakage vulnerability. An attacker can exploit this vulnerability by sending specific request packets to affected devices. Successful exploit may lead to information leakage. <b>CVE ID : CVE-2020-1827</b>	02-ipsec-en	
Improper Input Validation	17-02-2020	5	Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00; and Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00 have an input validation vulnerability where the IPSec module does not validate a field in a specific message. Attackers can send specific message to cause out-of-bound read, compromising normal service. <b>CVE ID : CVE-2020-1828</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-01-ipsec-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-01-ipsec-en</a>	O-HUA-USG9-050320/1319
Double Free	17-02-2020	5	Huawei NIP6800 versions V500R001C30 and V500R001C60SPC500; and Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, and V500R001C60SPC500 have a vulnerability that the IPSec module handles a message	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-03-ipsec-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-03-ipsec-en</a>	O-HUA-USG9-050320/1320

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improperly. Attackers can send specific message to cause double free memory. This may compromise normal service. <b>CVE ID : CVE-2020-1829</b>		
Out-of-bounds Read	18-02-2020	5	Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00; Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00 have a vulnerability that a memory management error exists when IPSec Module handing a specific message. This causes 1 byte out-of-bound read, compromising normal service. <b>CVE ID : CVE-2020-1830</b>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-04-ipsec-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200212-04-ipsec-en</a>	O-HUA-USG9-050320/1321
Information Exposure	17-02-2020	5	Huawei NGFW Module, NIP6300, NIP6600, Secospace USG6500, Secospace USG6600, and USG9500 versions V500R001C30, V500R001C60, and V500R005C00 have an information leakage vulnerability. An attacker can exploit this vulnerability by sending specific request packets to affected devices. Successful exploit may lead to information leakage.	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-firewall-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-firewall-en</a>	O-HUA-USG9-050320/1322

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-1856</b>		
Information Exposure	17-02-2020	2.1	<p>Huawei NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00SPC100; and Secospace USG6600 and USG9500 versions V500R001C30SPC200, V500R001C30SPC600, V500R001C60SPC500, and V500R005C00SPC100 have an information leakage vulnerability. Due to improper processing of some data, a local authenticated attacker can exploit this vulnerability through a series of operations. Successful exploitation may cause information leakage.</p> <p><b>CVE ID : CVE-2020-1857</b></p>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-leakage-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-leakage-en</a>	O-HUA-USG9-050320/1323
N/A	17-02-2020	5	<p>Huawei products NIP6800 versions V500R001C30, V500R001C60SPC500, and V500R005C00SPC100; Secospace USG6600 versions V500R001C30SPC600, V500R001C60SPC500, and V500R005C00SPC100; and USG9500 versions V500R001C30SPC600, V500R001C60SPC500, and V500R005C00SPC100 have a denial of service vulnerability. Attackers need to perform a series of operations in a special scenario to exploit this vulnerability. Successful</p>	<a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-dos-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200205-01-dos-en</a> , <a href="http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200219-04-dos-en">http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200219-04-dos-en</a>	O-HUA-USG9-050320/1324

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit may cause the new connections can't be established, result in a denial of service. <b>CVE ID : CVE-2020-1858</b>		
Access of Uninitialized Pointer	28-02-2020	4.9	NIP6800;Secospace USG6600;USG9500 products versions of V500R001C30; V500R001C60SPC500; V500R005C00SPC100 have a invalid pointer access vulnerability. The software system access an invalid pointer when operator logs in to the device and performs some operations. Successful exploit could cause certain process reboot. <b>CVE ID : CVE-2020-1874</b>	N/A	O-HUA-USG9-050320/1325
Access of Uninitialized Pointer	28-02-2020	4.9	NIP6800;Secospace USG6600;USG9500 with versions of V500R001C30; V500R001C60SPC500; V500R005C00SPC100 have an invalid pointer access vulnerability. The software system access an invalid pointer when administrator log in to the device and performs some operations. Successful exploit could cause certain process reboot. <b>CVE ID : CVE-2020-1877</b>	N/A	O-HUA-USG9-050320/1326
Uncontrolled Resource Consumption	28-02-2020	5	NIP6800;Secospace USG6600;USG9500 products with versions of V500R001C30; V500R001C60SPC500; V500R005C00SPC100 have	N/A	O-HUA-USG9-050320/1327

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>have a resource management error vulnerability. An attacker needs to perform specific operations to trigger a function of the affected device. Due to improper resource management of the function, the vulnerability can be exploited to cause service abnormal on affected devices.</p> <p><b>CVE ID : CVE-2020-1881</b></p>		
<b>IBM</b>					
<b>AIX</b>					
Uncontrolled Resource Consumption	19-02-2020	5	<p>IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow an unauthenticated user to send specially crafted packets to cause a denial of service from excessive memory usage.</p> <p><b>CVE ID : CVE-2020-4135</b></p>	<a href="https://www.ibm.com/support/pages/node/2876307">https://www.ibm.com/support/pages/node/2876307</a>	O-IBM-AIX-050320/1328
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-02-2020	4	<p>IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.5 could allow an authenticated attacker to cause a denial of service due to incorrect handling of certain commands. IBM X-Force ID: 174341.</p> <p><b>CVE ID : CVE-2020-4161</b></p>	<a href="https://www.ibm.com/support/pages/node/2874621">https://www.ibm.com/support/pages/node/2874621</a>	O-IBM-AIX-050320/1329
N/A	19-02-2020	4	<p>IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 10.5, 11.1, and 11.5 could allow an</p>	<a href="https://www.ibm.com/support/pages/node/2874621">https://www.ibm.com/support/pages/node/2874621</a>	O-IBM-AIX-050320/1330

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated attacker to send specially crafted commands to cause a denial of service. IBM X-Force ID: 174914. <b>CVE ID : CVE-2020-4200</b>	875251	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-02-2020	7.2	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 is vulnerable to a buffer overflow, caused by improper bounds checking which could allow a local attacker to execute arbitrary code on the system with root privileges. IBM X-Force ID: 174960. <b>CVE ID : CVE-2020-4204</b>	<a href="https://www.ibm.com/support/pages/node/2875875">https://www.ibm.com/support/pages/node/2875875</a>	O-IBM-AIX-050320/1331
Improper Privilege Management	19-02-2020	4.6	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.1 and 11.5 is vulnerable to an escalation of privilege when an authenticated local attacker with special permissions executes specially crafted Db2 commands. IBM X-Force ID: 175212. <b>CVE ID : CVE-2020-4230</b>	<a href="https://www.ibm.com/support/pages/node/2878809">https://www.ibm.com/support/pages/node/2878809</a>	O-IBM-AIX-050320/1332
<b>iteris</b>					
<b>vantage_velocity_firmware</b>					
Improper Neutralization of Special Elements used in an OS Command	17-02-2020	10	Iteris Vantage Velocity Field Unit 2.3.1, 2.4.2, and 3.0 devices allow the injection of OS commands into cgi-bin/timeconfig.py via shell metacharacters in the NTP	N/A	O-ITE-VANT-050320/1333

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			Server field. <b>CVE ID : CVE-2020-9020</b>		
Insufficiently Protected Credentials	17-02-2020	7.5	Iteris Vantage Velocity Field Unit 2.3.1 and 2.4.2 devices have two users that are not documented and are configured with weak passwords (User bluetooth, password bluetooth; User eclipse, password eclipse). Also, bluetooth is the root password. <b>CVE ID : CVE-2020-9023</b>	N/A	O-ITE-VANT-050320/1334
Improper Privilege Management	17-02-2020	10	Iteris Vantage Velocity Field Unit 2.3.1 and 2.4.2 devices have world-writable permissions for the /root/cleardata.pl (executed as root by crond) and /root/loadperl.sh (executed as root at boot time) scripts. <b>CVE ID : CVE-2020-9024</b>	N/A	O-ITE-VANT-050320/1335
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-02-2020	4.3	Iteris Vantage Velocity Field Unit 2.4.2 devices have multiple stored XSS issues in all parameters of the Start Data Viewer feature of the /cgi-bin/loaddata.py script. <b>CVE ID : CVE-2020-9025</b>	N/A	O-ITE-VANT-050320/1336
<b>Linux</b>					
<b>linux_kernel</b>					
Uncontrolled Resource Consumption	19-02-2020	5	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow an unauthenticated user to send specially crafted	<a href="https://www.ibm.com/support/pages/node/2876307">https://www.ibm.com/support/pages/node/2876307</a>	O-LIN-LINU-050320/1337

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			packets to cause a denial of service from excessive memory usage. <b>CVE ID : CVE-2020-4135</b>		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-02-2020	4	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.5 could allow an authenticated attacker to cause a denial of service due to incorrect handling of certain commands. IBM X-Force ID: 174341. <b>CVE ID : CVE-2020-4161</b>	<a href="https://www.ibm.com/support/pages/node/2874621">https://www.ibm.com/support/pages/node/2874621</a>	O-LIN-LINU-050320/1338
N/A	19-02-2020	4	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 10.5, 11.1, and 11.5 could allow an authenticated attacker to send specially crafted commands to cause a denial of service. IBM X-Force ID: 174914. <b>CVE ID : CVE-2020-4200</b>	<a href="https://www.ibm.com/support/pages/node/2875251">https://www.ibm.com/support/pages/node/2875251</a>	O-LIN-LINU-050320/1339
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-02-2020	7.2	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 is vulnerable to a buffer overflow, caused by improper bounds checking which could allow a local attacker to execute arbitrary code on the system with root privileges. IBM X-Force ID: 174960. <b>CVE ID : CVE-2020-4204</b>	<a href="https://www.ibm.com/support/pages/node/2875875">https://www.ibm.com/support/pages/node/2875875</a>	O-LIN-LINU-050320/1340
Improper Neutralization	24-02-2020	10	IBM Spectrum Protect Plus 10.1.0 and 10.1.5 could allow	<a href="https://www.ibm.com/">https://www.ibm.com/</a>	O-LIN-LINU-

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements in Output Used by a Downstream Component ('Injection')			a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. IBM X-Force ID: 175020. <b>CVE ID : CVE-2020-4210</b>	support/pages/node/3178863	050320/1341
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	24-02-2020	10	IBM Spectrum Protect Plus 10.1.0 and 10.1.5 could allow a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. IBM X-Force ID: 175022. <b>CVE ID : CVE-2020-4211</b>	<a href="https://www.ibm.com/support/pages/node/3178863">https://www.ibm.com/support/pages/node/3178863</a>	O-LIN-LINU-050320/1342
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	24-02-2020	10	IBM Spectrum Protect Plus 10.1.0 and 10.1.5 could allow a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. IBM X-Force ID: 175023. <b>CVE ID : CVE-2020-4212</b>	<a href="https://www.ibm.com/support/pages/node/3178863">https://www.ibm.com/support/pages/node/3178863</a>	O-LIN-LINU-050320/1343
Improper Privilege Management	19-02-2020	4.6	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.1 and 11.5 is vulnerable to an escalation of privilege when	<a href="https://www.ibm.com/support/pages/node/2878809">https://www.ibm.com/support/pages/node/2878809</a>	O-LIN-LINU-050320/1344

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an authenticated local attacker with special permissions executes specially crafted Db2 commands. IBM X-Force ID: 175212. <b>CVE ID : CVE-2020-4230</b>		
Out-of-bounds Read	25-02-2020	3.6	An issue was discovered in the Linux kernel through 5.5.6. set_fdc in drivers/block/floppy.c leads to a wait_til_ready out-of-bounds read because the FDC index is not checked for errors before assigning it, aka CID-2e90ca68b0d2. <b>CVE ID : CVE-2020-9383</b>	N/A	O-LIN-LINU-050320/1345

### Microchip

### syncserver\_s100\_firmware

Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-02-2020	4.3	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow stored XSS via the newUserName parameter on the "User Creation, Deletion and Password Maintenance" screen (when creating a new user). <b>CVE ID : CVE-2020-9028</b>	N/A	O-MIC-SYNC-050320/1346
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to messagelog.php. <b>CVE ID : CVE-2020-9029</b>	N/A	O-MIC-SYNC-050320/1347

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to the syslog.php. <b>CVE ID : CVE-2020-9030</b>	N/A	O-MIC-SYNC-050320/1348
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to daemonlog.php. <b>CVE ID : CVE-2020-9031</b>	N/A	O-MIC-SYNC-050320/1349
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to kernlog.php. <b>CVE ID : CVE-2020-9032</b>	N/A	O-MIC-SYNC-050320/1350
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to authlog.php. <b>CVE ID : CVE-2020-9033</b>	N/A	O-MIC-SYNC-050320/1351
Improper Input Validation	17-02-2020	5	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices mishandle session validation, leading to unauthenticated creation,	N/A	O-MIC-SYNC-050320/1352

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			modification, or elimination of users. <b>CVE ID : CVE-2020-9034</b>		
<b>syncserver_s200_firmware</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-02-2020	4.3	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow stored XSS via the newUserName parameter on the "User Creation, Deletion and Password Maintenance" screen (when creating a new user). <b>CVE ID : CVE-2020-9028</b>	N/A	O-MIC-SYNC-050320/1353
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to messagelog.php. <b>CVE ID : CVE-2020-9029</b>	N/A	O-MIC-SYNC-050320/1354
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to the syslog.php. <b>CVE ID : CVE-2020-9030</b>	N/A	O-MIC-SYNC-050320/1355
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to daemonlog.php.	N/A	O-MIC-SYNC-050320/1356

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			<b>CVE ID : CVE-2020-9031</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to kernlog.php. <b>CVE ID : CVE-2020-9032</b>	N/A	O-MIC-SYNC-050320/1357
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to authlog.php. <b>CVE ID : CVE-2020-9033</b>	N/A	O-MIC-SYNC-050320/1358
Improper Input Validation	17-02-2020	5	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices mishandle session validation, leading to unauthenticated creation, modification, or elimination of users. <b>CVE ID : CVE-2020-9034</b>	N/A	O-MIC-SYNC-050320/1359
<b>syncserver_s250_firmware</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-02-2020	4.3	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow stored XSS via the newUserName parameter on the "User Creation, Deletion and Password Maintenance" screen (when creating a new user).	N/A	O-MIC-SYNC-050320/1360

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<b>CVE ID : CVE-2020-9028</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to messagelog.php. <b>CVE ID : CVE-2020-9029</b>	N/A	O-MIC-SYNC-050320/1361
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to the syslog.php. <b>CVE ID : CVE-2020-9030</b>	N/A	O-MIC-SYNC-050320/1362
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to daemonlog.php. <b>CVE ID : CVE-2020-9031</b>	N/A	O-MIC-SYNC-050320/1363
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to kernlog.php. <b>CVE ID : CVE-2020-9032</b>	N/A	O-MIC-SYNC-050320/1364
Improper Limitation of a Pathname to a Restricted	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the	N/A	O-MIC-SYNC-050320/1365

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			FileName parameter to authlog.php. <b>CVE ID : CVE-2020-9033</b>		
Improper Input Validation	17-02-2020	5	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices mishandle session validation, leading to unauthenticated creation, modification, or elimination of users. <b>CVE ID : CVE-2020-9034</b>	N/A	O-MIC-SYNC-050320/1366
<b>syncserver_s300_firmware</b>					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-02-2020	4.3	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow stored XSS via the newUserName parameter on the "User Creation, Deletion and Password Maintenance" screen (when creating a new user). <b>CVE ID : CVE-2020-9028</b>	N/A	O-MIC-SYNC-050320/1367
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to messagelog.php. <b>CVE ID : CVE-2020-9029</b>	N/A	O-MIC-SYNC-050320/1368
Improper Limitation of a Pathname to a Restricted	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the	N/A	O-MIC-SYNC-050320/1369

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			FileName parameter to the syslog.php. <b>CVE ID : CVE-2020-9030</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to daemonlog.php. <b>CVE ID : CVE-2020-9031</b>	N/A	O-MIC-SYNC-050320/1370
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to kernlog.php. <b>CVE ID : CVE-2020-9032</b>	N/A	O-MIC-SYNC-050320/1371
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to authlog.php. <b>CVE ID : CVE-2020-9033</b>	N/A	O-MIC-SYNC-050320/1372
Improper Input Validation	17-02-2020	5	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices mishandle session validation, leading to unauthenticated creation, modification, or elimination of users. <b>CVE ID : CVE-2020-9034</b>	N/A	O-MIC-SYNC-050320/1373
<b>syncserver_s350_firmware</b>					

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-02-2020	4.3	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow stored XSS via the newUserName parameter on the "User Creation, Deletion and Password Maintenance" screen (when creating a new user). <b>CVE ID : CVE-2020-9028</b>	N/A	O-MIC-SYNC-050320/1374
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to messagelog.php. <b>CVE ID : CVE-2020-9029</b>	N/A	O-MIC-SYNC-050320/1375
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to the syslog.php. <b>CVE ID : CVE-2020-9030</b>	N/A	O-MIC-SYNC-050320/1376
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to daemonlog.php. <b>CVE ID : CVE-2020-9031</b>	N/A	O-MIC-SYNC-050320/1377
Improper Limitation of a Pathname to a	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow	N/A	O-MIC-SYNC-050320/1378

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			Directory Traversal via the FileName parameter to kernlog.php. <b>CVE ID : CVE-2020-9032</b>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-02-2020	6.4	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices allow Directory Traversal via the FileName parameter to authlog.php. <b>CVE ID : CVE-2020-9033</b>	N/A	O-MIC-SYNC-050320/1379
Improper Input Validation	17-02-2020	5	Symmetricon SyncServer S100 2.90.70.3, S200 1.30, S250 1.25, S300 2.65.0, and S350 2.80.1 devices mishandle session validation, leading to unauthenticated creation, modification, or elimination of users. <b>CVE ID : CVE-2020-9034</b>	N/A	O-MIC-SYNC-050320/1380
<b>Microsoft</b>					
<b>windows</b>					
Improper Input Validation	19-02-2020	7.5	vRealize Operations for Horizon Adapter (6.7.x prior to 6.7.1 and 6.6.x prior to 6.6.1) uses a JMX RMI service which is not securely configured. An unauthenticated remote attacker who has network access to vRealize Operations, with the Horizon Adapter running, may be able to execute arbitrary code in vRealize Operations. <b>CVE ID : CVE-2020-3943</b>	<a href="https://www.vmware.com/security/advisories/VMSA-2020-0003.html">https://www.vmware.com/security/advisories/VMSA-2020-0003.html</a>	O-MIC-WIND-050320/1381

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unquoted Search Path or Element	17-02-2020	1.9	Unquoted service executable path in DXL Broker in McAfee Data eXchange Layer (DXL) Framework 6.0.0 and earlier allows local users to cause a denial of service and malicious file execution via carefully crafted and named executable files. <b>CVE ID : CVE-2020-7252</b>	<a href="https://kc.mcafee.com/corporate/index?page=content&amp;id=SB10307">https://kc.mcafee.com/corporate/index?page=content&amp;id=SB10307</a>	O-MIC-WIND-050320/1382
Out-of-bounds Write	20-02-2020	10	Adobe Media Encoder versions 14.0 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . <b>CVE ID : CVE-2020-3764</b>	<a href="https://helpx.adobe.com/security/products/media-encoder/apsb20-10.html">https://helpx.adobe.com/security/products/media-encoder/apsb20-10.html</a>	O-MIC-WIND-050320/1383
Out-of-bounds Write	20-02-2020	10	Adobe After Effects versions 16.1.2 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. <b>CVE ID : CVE-2020-3765</b>	<a href="https://helpx.adobe.com/security/products/after_effects/apsb20-09.html">https://helpx.adobe.com/security/products/after_effects/apsb20-09.html</a>	O-MIC-WIND-050320/1384
Improper Authentication	19-02-2020	5	vRealize Operations for Horizon Adapter (6.7.x prior to 6.7.1 and 6.6.x prior to 6.6.1) has an improper trust store configuration leading to authentication bypass. An unauthenticated remote attacker who has network access to vRealize Operations, with the Horizon Adapter running, may be able to bypass Adapter authentication. <b>CVE ID : CVE-2020-3944</b>	<a href="https://www.vmware.com/security/advisories/VMSA-2020-0003.html">https://www.vmware.com/security/advisories/VMSA-2020-0003.html</a>	O-MIC-WIND-050320/1385

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	19-02-2020	5	vRealize Operations for Horizon Adapter (6.7.x prior to 6.7.1 and 6.6.x prior to 6.6.1) contains an information disclosure vulnerability due to incorrect pairing implementation between the vRealize Operations for Horizon Adapter and Horizon View. An unauthenticated remote attacker who has network access to vRealize Operations, with the Horizon Adapter running, may obtain sensitive information <b>CVE ID : CVE-2020-3945</b>	<a href="https://www.vmware.com/security/advisories/VMSA-2020-0003.html">https://www.vmware.com/security/advisories/VMSA-2020-0003.html</a>	O-MIC-WIND-050320/1386
Uncontrolled Resource Consumption	19-02-2020	5	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow an unauthenticated user to send specially crafted packets to cause a denial of service from excessive memory usage. <b>CVE ID : CVE-2020-4135</b>	<a href="https://www.ibm.com/support/pages/node/2876307">https://www.ibm.com/support/pages/node/2876307</a>	O-MIC-WIND-050320/1387
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-02-2020	4	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.5 could allow an authenticated attacker to cause a denial of service due to incorrect handling of certain commands. IBM X-Force ID: 174341. <b>CVE ID : CVE-2020-4161</b>	<a href="https://www.ibm.com/support/pages/node/2874621">https://www.ibm.com/support/pages/node/2874621</a>	O-MIC-WIND-050320/1388
N/A	19-02-2020	4	IBM DB2 for Linux, UNIX and	<a href="https://www">https://www</a>	O-MIC-WIND-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Windows (includes DB2 Connect Server) 10.5, 11.1, and 11.5 could allow an authenticated attacker to send specially crafted commands to cause a denial of service. IBM X-Force ID: 174914. <b>CVE ID : CVE-2020-4200</b>	w.ibm.com/support/pages/node/2875251	050320/1389
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-02-2020	7.2	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 is vulnerable to a buffer overflow, caused by improper bounds checking which could allow a local attacker to execute arbitrary code on the system with root privileges. IBM X-Force ID: 174960. <b>CVE ID : CVE-2020-4204</b>	<a href="https://www.ibm.com/support/pages/node/2875875">https://www.ibm.com/support/pages/node/2875875</a>	O-MIC-WIND-050320/1390
Improper Privilege Management	19-02-2020	4.6	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.1 and 11.5 is vulnerable to an escalation of privilege when an authenticated local attacker with special permissions executes specially crafted Db2 commands. IBM X-Force ID: 175212. <b>CVE ID : CVE-2020-4230</b>	<a href="https://www.ibm.com/support/pages/node/2878809">https://www.ibm.com/support/pages/node/2878809</a>	O-MIC-WIND-050320/1391
Out-of-bounds Read	27-02-2020	6.4	In PHP versions 7.3.x below 7.3.15 and 7.4.x below 7.4.3, while extracting PHAR files on Windows using phar extension, certain content	N/A	O-MIC-WIND-050320/1392

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			inside PHAR file could lead to one-byte read past the allocated buffer. This could potentially lead to information disclosure or crash. <b>CVE ID : CVE-2020-7061</b>		
Uncontrolled Search Path Element	20-02-2020	4.6	Trend Micro Vulnerability Protection 2.0 is affected by a vulnerability that could allow an attack to use the product installer to load other DLL files located in the same directory. <b>CVE ID : CVE-2020-8601</b>	N/A	O-MIC-WIND-050320/1393
Improper Preservation of Permissions	28-02-2020	7.2	OpenVPN Connect 3.1.0.361 on Windows has Insecure Permissions for %PROGRAMDATA%\OpenVPN Connect\drivers\tap\amd64\win10, which allows local users to gain privileges by copying a malicious drvstore.dll there. <b>CVE ID : CVE-2020-9442</b>	N/A	O-MIC-WIND-050320/1394
<b>NEC</b>					
<b>aterm_wf1200c_firmware</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-02-2020	8.3	Aterm series (Aterm WF1200C firmware Ver1.2.1 and earlier, Aterm WG1200CR firmware Ver1.2.1 and earlier, Aterm WG2600HS firmware Ver1.3.2 and earlier) allows an attacker on the same network segment to execute arbitrary OS commands with root privileges via UPnP	N/A	O-NEC-ATER-050320/1395

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			function. <b>CVE ID : CVE-2020-5524</b>		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-02-2020	7.7	Aterm series (Aterm WF1200C firmware Ver1.2.1 and earlier, Aterm WG1200CR firmware Ver1.2.1 and earlier, Aterm WG2600HS firmware Ver1.3.2 and earlier) allows an authenticated attacker on the same network segment to execute arbitrary OS commands with root privileges via management screen. <b>CVE ID : CVE-2020-5525</b>	N/A	O-NEC-ATER-050320/1396
<b>aterm_wg1200cr_firmware</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-02-2020	8.3	Aterm series (Aterm WF1200C firmware Ver1.2.1 and earlier, Aterm WG1200CR firmware Ver1.2.1 and earlier, Aterm WG2600HS firmware Ver1.3.2 and earlier) allows an attacker on the same network segment to execute arbitrary OS commands with root privileges via UPnP function. <b>CVE ID : CVE-2020-5524</b>	N/A	O-NEC-ATER-050320/1397
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-02-2020	7.7	Aterm series (Aterm WF1200C firmware Ver1.2.1 and earlier, Aterm WG1200CR firmware Ver1.2.1 and earlier, Aterm WG2600HS firmware Ver1.3.2 and earlier) allows an authenticated attacker on the same network segment	N/A	O-NEC-ATER-050320/1398

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary OS commands with root privileges via management screen. <b>CVE ID : CVE-2020-5525</b>		
<b>aterm_wg2600hs_firmware</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-02-2020	8.3	Aterm series (Aterm WF1200C firmware Ver1.2.1 and earlier, Aterm WG1200CR firmware Ver1.2.1 and earlier, Aterm WG2600HS firmware Ver1.3.2 and earlier) allows an attacker on the same network segment to execute arbitrary OS commands with root privileges via UPnP function. <b>CVE ID : CVE-2020-5524</b>	N/A	O-NEC-ATER-050320/1399
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-02-2020	7.7	Aterm series (Aterm WF1200C firmware Ver1.2.1 and earlier, Aterm WG1200CR firmware Ver1.2.1 and earlier, Aterm WG2600HS firmware Ver1.3.2 and earlier) allows an authenticated attacker on the same network segment to execute arbitrary OS commands with root privileges via management screen. <b>CVE ID : CVE-2020-5525</b>	N/A	O-NEC-ATER-050320/1400
Improper Neutralization of Input During Web Page Generation	21-02-2020	4.3	Cross-site scripting vulnerability in Aterm WG2600HS firmware Ver1.3.2 and earlier allows remote attackers to inject arbitrary web script or	N/A	O-NEC-ATER-050320/1401

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			HTML via unspecified vectors. <b>CVE ID : CVE-2020-5533</b>		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-02-2020	7.7	Aterm WG2600HS firmware Ver1.3.2 and earlier allows an authenticated attacker on the same network segment to execute arbitrary OS commands with root privileges via unspecified vectors. <b>CVE ID : CVE-2020-5534</b>	N/A	O-NEC-ATER-050320/1402
<b>Opensuse</b>					
<b>leap</b>					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	4.3	A denial of service issue was addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. A malicious website may be able to cause a denial of service. <b>CVE ID : CVE-2020-3862</b>	N/A	O-OPE-LEAP-050320/1403
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted web content may lead to arbitrary code	N/A	O-OPE-LEAP-050320/1404

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. <b>CVE ID : CVE-2020-3865</b>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-02-2020	4.3	A logic issue was addressed with improved state management. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted web content may lead to universal cross site scripting. <b>CVE ID : CVE-2020-3867</b>	N/A	O-OPE-LEAP-050320/1405
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-02-2020	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted web content may lead to arbitrary code execution. <b>CVE ID : CVE-2020-3868</b>	N/A	O-OPE-LEAP-050320/1406
<b>Phoenixcontact</b>					
<b>ilc_2050_bi_firmware</b>					
Incorrect Permission Assignment for Critical Resource	17-02-2020	7.5	An issue was discovered on Phoenix Contact Emalytics Controller ILC 2050 BI before 1.2.3 and BI-L before 1.2.3 devices. There is an insecure mechanism for read and write access to the configuration of the device.	N/A	O-PHO-ILC_-050320/1407

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			The mechanism can be discovered by examining a link on the website of the device. <b>CVE ID : CVE-2020-8768</b>		
<b>ilc_2050_bi-l_firmware</b>					
Incorrect Permission Assignment for Critical Resource	17-02-2020	7.5	An issue was discovered on Phoenix Contact Emalytics Controller ILC 2050 BI before 1.2.3 and BI-L before 1.2.3 devices. There is an insecure mechanism for read and write access to the configuration of the device. The mechanism can be discovered by examining a link on the website of the device. <b>CVE ID : CVE-2020-8768</b>	N/A	O-PHO-ILC_-050320/1408
<b>Postoaktraffic</b>					
<b>awam_bluetooth_field_device_firmware</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-02-2020	10	Post Oak AWAM Bluetooth Field Device 7400v2.08.21.2018, 7800SD.2015.1.16, 2011.3, 7400v2.02.01.2019, and 7800SD.2012.12.5 is vulnerable to injections of operating system commands through timeconfig.py via shell metacharacters in the htmlNtpServer parameter. <b>CVE ID : CVE-2020-9021</b>	N/A	O-POS-AWAM-050320/1409
<b>tonnet</b>					
<b>tat-71416g1_firmware</b>					
Incorrect Authorizatio	27-02-2020	10	DVR firmware in TAT-76 and TAT-77 series of products, provided by	<a href="https://tvn.twcert.org.tw/taiwanvn">https://tvn.twcert.org.tw/taiwanvn</a>	O-TON-TAT--050320/1410

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			TONNET, contain misconfigured authentication mechanism. Attackers can crack the default password and gain access to the system. <b>CVE ID : CVE-2020-3923</b>	/TVN-201910003, <a href="https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2bbcf">https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2bbcf</a>	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	27-02-2020	10	DVR firmware in TAT-76 and TAT-77 series of products, provided by TONNET do not properly verify patch files. Attackers can inject a specific command into a patch file and gain access to the system. <b>CVE ID : CVE-2020-3924</b>	<a href="https://tvn.twcert.org.tw/taiwanvn/TVN-201910004,https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2bbcf">https://tvn.twcert.org.tw/taiwanvn/TVN-201910004,https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2bbcf</a>	O-TON-TAT--050320/1411
<b>tat-71832g1_firmware</b>					
Incorrect Authorization	27-02-2020	10	DVR firmware in TAT-76 and TAT-77 series of products, provided by TONNET, contain misconfigured authentication mechanism. Attackers can crack the default password and gain access to the system. <b>CVE ID : CVE-2020-3923</b>	<a href="https://tvn.twcert.org.tw/taiwanvn/TVN-201910003,https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2bbcf">https://tvn.twcert.org.tw/taiwanvn/TVN-201910003,https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2bbcf</a>	O-TON-TAT--050320/1412
Improper Neutralization of Special	27-02-2020	10	DVR firmware in TAT-76 and TAT-77 series of products, provided by	<a href="https://tvn.twcert.org.tw/taiwanvn">https://tvn.twcert.org.tw/taiwanvn</a>	O-TON-TAT--050320/1413

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements in Output Used by a Downstream Component ('Injection')			TONNET do not properly verify patch files. Attackers can inject a specific command into a patch file and gain access to the system. <b>CVE ID : CVE-2020-3924</b>	/TVN-201910004, <a href="https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2bbcf">https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2bbcf</a>	
<b>tat-76104g3_firmware</b>					
Incorrect Authorization	27-02-2020	10	DVR firmware in TAT-76 and TAT-77 series of products, provided by TONNET, contain misconfigured authentication mechanism. Attackers can crack the default password and gain access to the system. <b>CVE ID : CVE-2020-3923</b>	<a href="https://tvn.twcert.org.tw/taiwanvn/TVN-201910003,https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2bbcf">https://tvn.twcert.org.tw/taiwanvn/TVN-201910003,https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2bbcf</a>	O-TON-TAT--050320/1414
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	27-02-2020	10	DVR firmware in TAT-76 and TAT-77 series of products, provided by TONNET do not properly verify patch files. Attackers can inject a specific command into a patch file and gain access to the system. <b>CVE ID : CVE-2020-3924</b>	<a href="https://tvn.twcert.org.tw/taiwanvn/TVN-201910004,https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2bbcf">https://tvn.twcert.org.tw/taiwanvn/TVN-201910004,https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2bbcf</a>	O-TON-TAT--050320/1415
<b>tat-76108g3_firmware</b>					
Incorrect Authorization	27-02-2020	10	DVR firmware in TAT-76 and TAT-77 series of	<a href="https://tvn.twcert.org.t">https://tvn.twcert.org.t</a>	O-TON-TAT--

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			products, provided by TONNET, contain misconfigured authentication mechanism. Attackers can crack the default password and gain access to the system. <b>CVE ID : CVE-2020-3923</b>	w/taiwanvn/tvn-201910003, https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2bbcf	050320/1416
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	27-02-2020	10	DVR firmware in TAT-76 and TAT-77 series of products, provided by TONNET do not properly verify patch files. Attackers can inject a specific command into a patch file and gain access to the system. <b>CVE ID : CVE-2020-3924</b>	https://tvn.twcert.org.tw/taiwanvn/tvn-201910004, https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2bbcf	O-TON-TAT--050320/1417
<b>tat-76116g3_firmware</b>					
Incorrect Authorization	27-02-2020	10	DVR firmware in TAT-76 and TAT-77 series of products, provided by TONNET, contain misconfigured authentication mechanism. Attackers can crack the default password and gain access to the system. <b>CVE ID : CVE-2020-3923</b>	https://tvn.twcert.org.tw/taiwanvn/tvn-201910003, https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2bbcf	O-TON-TAT--050320/1418
Improper Neutralization	27-02-2020	10	DVR firmware in TAT-76 and TAT-77 series of	https://tvn.twcert.org.t	O-TON-TAT--050320/1419

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements in Output Used by a Downstream Component ('Injection')			products, provided by TONNET do not properly verify patch files. Attackers can inject a specific command into a patch file and gain access to the system. <b>CVE ID : CVE-2020-3924</b>	w/taiwanvn/TVN-201910004, <a href="https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2bbcf">https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2bbcf</a>	
<b>tat-76132g3_firmware</b>					
Incorrect Authorization	27-02-2020	10	DVR firmware in TAT-76 and TAT-77 series of products, provided by TONNET, contain misconfigured authentication mechanism. Attackers can crack the default password and gain access to the system. <b>CVE ID : CVE-2020-3923</b>	<a href="https://tvn.twcert.org.tw/taiwanvn/TVN-201910003,https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2bbcf">https://tvn.twcert.org.tw/taiwanvn/TVN-201910003,https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2bbcf</a>	O-TON-TAT--050320/1420
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	27-02-2020	10	DVR firmware in TAT-76 and TAT-77 series of products, provided by TONNET do not properly verify patch files. Attackers can inject a specific command into a patch file and gain access to the system. <b>CVE ID : CVE-2020-3924</b>	<a href="https://tvn.twcert.org.tw/taiwanvn/TVN-201910004,https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2bbcf">https://tvn.twcert.org.tw/taiwanvn/TVN-201910004,https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2bbcf</a>	O-TON-TAT--050320/1421
<b>tat-77104g1_firmware</b>					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	27-02-2020	10	DVR firmware in TAT-76 and TAT-77 series of products, provided by TONNET, contain misconfigured authentication mechanism. Attackers can crack the default password and gain access to the system. <b>CVE ID : CVE-2020-3923</b>	<a href="https://tvn.twcert.org.tw/taiwanvn/TVN-201910003">https://tvn.twcert.org.tw/taiwanvn/TVN-201910003</a> , <a href="https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2bbcf">https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2bbcf</a>	O-TON-TAT--050320/1422
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	27-02-2020	10	DVR firmware in TAT-76 and TAT-77 series of products, provided by TONNET do not properly verify patch files. Attackers can inject a specific command into a patch file and gain access to the system. <b>CVE ID : CVE-2020-3924</b>	<a href="https://tvn.twcert.org.tw/taiwanvn/TVN-201910004">https://tvn.twcert.org.tw/taiwanvn/TVN-201910004</a> , <a href="https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2bbcf">https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2bbcf</a>	O-TON-TAT--050320/1423
<b>tat-70432n_firmware</b>					
Incorrect Authorization	27-02-2020	10	DVR firmware in TAT-76 and TAT-77 series of products, provided by TONNET, contain misconfigured authentication mechanism. Attackers can crack the default password and gain access to the system. <b>CVE ID : CVE-2020-3923</b>	<a href="https://tvn.twcert.org.tw/taiwanvn/TVN-201910003">https://tvn.twcert.org.tw/taiwanvn/TVN-201910003</a> , <a href="https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2bbcf">https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2bbcf</a>	O-TON-TAT--050320/1424

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



Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	27-02-2020	10	DVR firmware in TAT-76 and TAT-77 series of products, provided by TONNET do not properly verify patch files. Attackers can inject a specific command into a patch file and gain access to the system. <b>CVE ID : CVE-2020-3924</b>	<a href="https://tvn.twcert.org.tw/taiwanvn/TVN-201910004">https://tvn.twcert.org.tw/taiwanvn/TVN-201910004</a> , <a href="https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2bbcf">https://www.chtsecurity.com/news/4ef5eb3a-fdc3-4d78-8dd7-ec7213e2bbcf</a>	O-TON-TAT--050320/1425
<b>Tp-link</b>					
<b>tl-wr849n_firmware</b>					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-02-2020	7.5	On TP-Link TL-WR849N 0.9.1 4.16 devices, a remote command execution vulnerability in the diagnostics area can be exploited when an attacker sends specific shell metacharacters to the panel's traceroute feature. <b>CVE ID : CVE-2020-9374</b>	N/A	O-TP--TL-W-050320/1426
<b>ZTE</b>					
<b>e8820v3_firmware</b>					
Incorrect Permission Assignment for Critical Resource	27-02-2020	3.3	ZTE E8820V3 router product is impacted by a permission and access control vulnerability. Attackers could use this vulnerability to tamper with DDNS parameters and send DoS attacks on the specified URL. <b>CVE ID : CVE-2020-6863</b>	<a href="http://support.zte.com.cn/support/news/LooPholeInfoDetail.aspx?newsId=1012382">http://support.zte.com.cn/support/news/LooPholeInfoDetail.aspx?newsId=1012382</a>	O-ZTE-E882-050320/1427
Information Exposure	27-02-2020	3.3	ZTE E8820V3 router product is impacted by an	<a href="http://support.zte.com">http://support.zte.com</a>	O-ZTE-E882-050320/1428

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>information leak vulnerability. Attackers could use this vulnerability to to gain wireless passwords. After obtaining the wireless password, the attacker could collect information and attack the router.</p> <p><b>CVE ID : CVE-2020-6864</b></p>	<p>cn/support/news/Loo pholeInfoD etail.aspx?n ewsId=101 2382</p>	

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