National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures(CVE) Report

01 - 15 Feb 2020 Vol. 07 No. 03

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
1up					
oneupuploaderbundle					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-02-2020	6.5	oneup/uploader-bundle before 1.9.3 and 2.1.5, can be exploited to upload files to arbitrary folders on the filesystem. The assembly process can further be misused with some restrictions to delete and copy files to other locations. This is fixed in versions 1.9.3 and 2.1.5. **CVE ID : CVE-2020-5237**	https://github.com/1up-lab/OneupUploaderBundle/security/advisories/GHSA-x8wj-6m73-gfqp	A-1UP-ONEU-180220/1
Adobe					
framemaker					
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3720**	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	A-ADO-FRAM-180220/2
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	A-ADO-FRAM-180220/3

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3721		
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3722**	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	A-ADO-FRAM-180220/4
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3723**	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	A-ADO-FRAM-180220/5
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3724**	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	A-ADO-FRAM-180220/6
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3725**	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	A-ADO-FRAM-180220/7
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have an out-of-bounds write vulnerability. Successful	https://helpx.adobe.com/security/products/framemaker/apsb	A-ADO-FRAM-180220/8

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3726**	20-04.html	
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3727**	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	A-ADO-FRAM-180220/9
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3728**	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	A-ADO-FRAM-180220/10
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3729**	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	A-ADO-FRAM-180220/11
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3730**	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	A-ADO-FRAM-180220/12
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have a heap	https://helpx.adobe.com/security/pr	A-ADO-FRAM-180220/13

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			overflow vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3731**	oducts/framemaker/apsb20-04.html	
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3732**	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	A-ADO-FRAM-180220/14
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3733**	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	A-ADO-FRAM-180220/15
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3734**	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	A-ADO-FRAM-180220/16
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3735**	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	A-ADO-FRAM-180220/17
Out-of-bounds	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and	https://helpx.adobe.com	A-ADO-FRAM-180220/18

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3736**	/security/products/framemaker/apsb20-04.html	
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3737**	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	A-ADO-FRAM-180220/19
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3738**	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	A-ADO-FRAM-180220/20
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3739**	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	A-ADO-FRAM-180220/21
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-02-2020	10	Adobe Framemaker versions 2019.0.4 and below have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3740**	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	A-ADO-FRAM-180220/22

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
agendaless					
waitress					
Uncontrolled Resource Consumption	04-02-2020	6.8	Waitress version 1.4.2 allows a DOS attack When waitress receives a header that contains invalid characters. When a header like "Bad-header: xxxxxxxxxxxxxxx\x10" is received, it will cause the regular expression engine to catastrophically backtrack causing the process to use 100% CPU time and blocking any other interactions. This allows an attacker to send a single request with an invalid header and take the service offline. This issue was introduced in version 1.4.2 when the regular expression was updated to attempt to match the behaviour required by errata associated with RFC7230. The regular expression that is used to validate incoming headers has been updated in version 1.4.3, it is recommended that people upgrade to the new version of Waitress as soon as possible. **CVE ID : CVE-2020-5236**	https://github.com/Pylons/waitress/security/advisories/GHSA-73m2-3pwg-5fgc	A-AGE-WAIT-180220/23
Artica					
pandora_fms					
Improper	12-02-2020	9	functions_netflow.php in	N/A	A-ART-PAND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in an OS Command ('OS Command Injection')			Artica Pandora FMS 7.0 allows remote attackers to execute arbitrary OS commands via shell metacharacters in the index.php?operation/netflow/nf_live_view ip_dst, dst_port, or src_port parameter, a different vulnerability than CVE-2019-20224. **CVE ID : CVE-2020-8947**		180220/24
Bestwebsoft					
htaccess					
Cross-Site Request Forgery (CSRF)	06-02-2020	6.8	The BestWebSoft Htaccess plugin through 1.8.1 for WordPress allows wp-admin/admin.php?page=htaccess.php&action=htaccess_editor CSRF. The flag htccss_nonce_name passes the nonce to WordPress but the plugin does not validate it correctly, resulting in a wrong implementation of anti-CSRF protection. In this way, an attacker is able to direct the victim to a malicious web page that modifies the .htaccess file, and takes control of the website. **CVE ID : CVE-2020-8658**	N/A	A-BES-HTAC-180220/25
biscom					
secure_file_transfer					
N/A	07-02-2020	7.5	Biscom Secure File Transfer (SFT) before 5.1.1071 and 6.0.1xxx	N/A	A-BIS-SECU-180220/26

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 6.0.1005 allows Remote Code Execution on the server. **CVE ID : CVE-2020-8796**		
bludit					
bludit					
Missing Authorization	07-02-2020	4	ajax/profile-picture-upload.php in Bludit 3.10.0 allows authenticated users to change other users' profile pictures. **CVE ID : CVE-2020-8811**	N/A	A-BLU-BLUD-180220/27
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-02-2020	3.5	** DISPUTED ** Bludit 3.10.0 allows Editor or Author roles to insert malicious JavaScript on the WYSIWYG editor. NOTE: the vendor's perspective is that this is "not a bug." **CVE ID : CVE-2020-8812**	N/A	A-BLU-BLUD-180220/28
bosch					
video_management_system					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-02-2020	5	A path traversal vulnerability in the Bosch Video Management System (BVMS) NoTouch deployment allows an unauthenticated remote attacker to read arbitrary files from the Central Server. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch BVMS Viewer versions 10.0 <= 10.0.0.1225, 9.0 <=	https://psirt.bosch.com/security-advisories/bosch-sa-815013-bt.html	A-BOS-VIDE-180220/29

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR IP all-in-one 5000 if a vulnerable BVMS version is installed. **CVE ID : CVE-2020-6768**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-02-2020	4	A path traversal vulnerability in the Bosch Video Management System (BVMS) FileTransferService allows an authenticated remote attacker to read arbitrary files from the Central Server. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch BVMS Viewer versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR IP all-in-one 5000 if a vulnerable BVMS version is installed. **CVE ID : CVE-2020-6767**	https://psirt.bosch.com/security-advisories/BOSCH-SA-381489-BT.html	A-BOS-VIDE-180220/30
video_management_system_viewer					
Improper Limitation of a Pathname to a Restricted Directory ('Path	07-02-2020	5	A path traversal vulnerability in the Bosch Video Management System (BVMS) NoTouch deployment allows an unauthenticated remote attacker to read arbitrary	https://psirt.bosch.com/security-advisories/bosch-sa-815013-	A-BOS-VIDE-180220/31

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			files from the Central Server. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch BVMS Viewer versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR IP all-in-one 5000 if a vulnerable BVMS version is installed. **CVE ID : CVE-2020-6768**	bt.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-02-2020	4	A path traversal vulnerability in the Bosch Video Management System (BVMS) FileTransferService allows an authenticated remote attacker to read arbitrary files from the Central Server. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch BVMS Viewer versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR IP all-in-one 5000 if a vulnerable BVMS version is installed.	https://psirt.bosch.com/security-advisories/BOSCH-SA-381489-BT.html	A-BOS-VIDE-180220/32

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-6767		
bosch_video_management_system_mobile_video_service					
Deserialization of Untrusted Data	07-02-2020	10	Deserialization of Untrusted Data in the BVMS Mobile Video Service (BVMS MVS) allows an unauthenticated remote attacker to execute arbitrary code on the system. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000 and DIVAR IP 7000 if a vulnerable BVMS version is installed. **CVE ID : CVE-2020-6770**	https://psirt.bosch.com/security-advisories/BOSCH-SA-885551-BT.html	A-BOS-BOSC-180220/33
video_streaming_gateway					
Missing Authentication for Critical Function	07-02-2020	6.4	Missing Authentication for Critical Function in the Bosch Video Streaming Gateway (VSG) allows an unauthenticated remote attacker to retrieve and set arbitrary configuration data of the Video Streaming Gateway. A successful attack can impact the confidentiality and availability of live and recorded video data of all cameras configured to be controlled by the VSG as well as the recording storage associated with the VSG. This affects Bosch Video Streaming Gateway versions 6.45 <= 6.45.08,	https://psirt.bosch.com/security-advisories/BOSCH-SA-260625-BT.html	A-BOS-VIDE-180220/34

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			6.44 <= 6.44.022, 6.43 <= 6.43.0023 and 6.42.10 and older. This affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR IP all-in-one 5000 if a vulnerable VSG version is installed with BVMS. This affects Bosch DIVAR IP 2000 <= 3.62.0019 and DIVAR IP 5000 <= 3.80.0039 if the corresponding port 8023 has been opened in the device's firewall. **CVE ID : CVE-2020-6769**		
Canonical					
cloud-init					
Use of Insufficiently Random Values	05-02-2020	2.1	cloud-init through 19.4 relies on Mersenne Twister for a random password, which makes it easier for attackers to predict passwords, because rand_str in cloudinit/util.py calls the random.choice function. **CVE ID : CVE-2020-8631**	N/A	A-CAN-CLOU-180220/35
Insufficiently Protected Credentials	05-02-2020	2.1	In cloud-init through 19.4, rand_user_password in cloudinit/config/cc_set_passwords.py has a small default pwlen value, which makes it easier for attackers to guess passwords. **CVE ID : CVE-2020-8632**	N/A	A-CAN-CLOU-180220/36
Ceph					
ceph					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	07-02-2020	6.8	A flaw was found in the way the Ceph RGW Beast front-end handles unexpected disconnects. An authenticated attacker can abuse this flaw by making multiple disconnect attempts resulting in a permanent leak of a socket connection by radosgw. This flaw could lead to a denial of service condition by pile up of CLOSE_WAIT sockets, eventually leading to the exhaustion of available resources, preventing legitimate users from connecting to the system. **CVE ID : CVE-2020-1700**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1700	A-CEP-CEPH-180220/37
changingtec					
servisign					
N/A	03-02-2020	9.3	A Remote Code Execution(RCE) vulnerability exists in some designated applications in ServiSign security plugin, as long as the interface is captured, attackers are able to launch RCE and executes arbitrary command on target system via malicious crafted scripts. **CVE ID : CVE-2020-3925**	https://tvn.twcert.org.tw/taiwanvn/TVN-201910005	A-CHA-SERV-180220/38
Files or Directories Accessible to	03-02-2020	7.8	An arbitrary-file-access vulnerability exists in ServiSign security plugin,	https://tvn.twcert.org.tw/taiwanvn/T	A-CHA-SERV-180220/39

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
External Parties			as long as the attackers learn the specific API function, they may access arbitrary files on target system via crafted API parameter. **CVE ID : CVE-2020-3926**	VN-201910006	
Files or Directories Accessible to External Parties	03-02-2020	8.5	An arbitrary-file-access vulnerability exists in ServiSign security plugin, as long as the attackers learn the specific API function, they may access arbitrary files on target system via crafted API parameter. **CVE ID : CVE-2020-3927**	https://tvn.twcert.org.tw/taiwanvn/TVN-201910007	A-CHA-SERV-180220/40
circl					
ail_framework					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-02-2020	5	Global.py in AIL framework 2.8 allows path traversal. **CVE ID : CVE-2020-8545**	N/A	A-CIR-AIL_-180220/41
Cisco					
identity_services_engine					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-02-2020	3.5	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) Software could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack on an affected	N/A	A-CIS-IDEN-180220/42

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. The vulnerability is due to insufficient input validation by the web-based management interface. An attacker could exploit this vulnerability by providing malicious data to a specific field within the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco ISE Software releases 2.7.0 and later contains the fix for this vulnerability. **CVE ID : CVE-2020-3149**		
ucs_manager					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol	N/A	A-CIS-UCS_-180220/43

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to	N/A	A-CIS-UCS_-180220/44

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
Clamav					
clamav					
Out-of-bounds Read	05-02-2020	5	A vulnerability in the Data-Loss-Prevention (DLP) module in Clam AntiVirus (ClamAV) Software versions 0.102.1 and 0.102.0 could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. The vulnerability is due to an out-of-bounds read affecting users that have enabled the optional DLP feature. An attacker could exploit this vulnerability by sending a crafted email file to an affected device. An exploit could allow the attacker to cause the ClamAV scanning process crash, resulting in a denial of service condition. **CVE ID : CVE-2020-3123**	https://blog.clamav.net/2020/02/clamav-01022-security-patch-released.html	A-CLA-CLAM-180220/45
Cmsjunkie					
j-businessdirectory					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	03-02-2020	4.3	The J-BusinessDirectory extension before 5.2.9 for Joomla! allows Reverse Tabnabbing. In some configurations, the link to the business website can be entered by any user. If it doesn't contain rel="noopener" (or similar attributes such as noreferrer), the tabnabbing may occur. To reproduce the bug, create a business with a website link that contains JavaScript to exploit the window.opener property (for example, by setting window.opener.location). **CVE ID : CVE-2020-5182**	https://www.cmsjunkie.com/blog/joomla_business_directory_5-2-9_release/	A-CMS-J-BU-180220/46
corsair					
icue					
Improper Privilege Management	07-02-2020	7.2	The CorsairLLAccess64.sys and CorsairLLAccess32.sys drivers in CORSAIR iCUE before 3.25.60 allow local non-privileged users (including low-integrity level processes) to read and write to arbitrary physical memory locations, and consequently gain NT AUTHORITY\SYSTEM privileges, via a function call such as MmMapIoSpace. **CVE ID : CVE-2020-8808**	N/A	A-COR-ICUE-180220/47
corusent					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
global_tv					
Information Exposure	05-02-2020	4	The Global TV application 2.3.2 for Android and 4.7.5 for iOS sends Unencrypted Analytics. **CVE ID : CVE-2020-8506**	N/A	A-COR-GLOB-180220/48
Dell					
emc_unity_operating_environment					
Improper Validation of Array Index	06-02-2020	7.8	Dell EMC Unity, Dell EMC Unity XT, and Dell EMC UnityVSA versions prior to 5.0.2.0.5.009 contain a Denial of Service vulnerability on NAS Server SSH implementation that is used to provide SFTP service on a NAS server. A remote unauthenticated attacker may potentially exploit this vulnerability and cause a Denial of Service (Storage Processor Panic) by sending an out of order SSH protocol sequence. **CVE ID : CVE-2020-5319**	N/A	A-DEL-EMC_-180220/49
emc_unityvsa_operating_environment					
Improper Validation of Array Index	06-02-2020	7.8	Dell EMC Unity, Dell EMC Unity XT, and Dell EMC UnityVSA versions prior to 5.0.2.0.5.009 contain a Denial of Service vulnerability on NAS Server SSH implementation that is used to provide SFTP service on a NAS server. A remote unauthenticated	N/A	A-DEL-EMC_-180220/50

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker may potentially exploit this vulnerability and cause a Denial of Service (Storage Processor Panic) by sending an out of order SSH protocol sequence. **CVE ID : CVE-2020-5319**		
emc_elastic_cloud_storage					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-02-2020	3.5	Dell EMC ECS versions prior to 3.4.0.1 contain an XSS vulnerability. A remote authenticated malicious user could exploit this vulnerability to store malicious HTML or JavaScript code in a trusted application data store. When victim users access the data store through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable web application. **CVE ID : CVE-2020-5317**	N/A	A-DEL-EMC_-180220/51
emc_isilon_onefs					
Incorrect Authorization	06-02-2020	5	Dell EMC Isilon OneFS versions 8.1.2, 8.1.0.4, 8.1.0.3, and 8.0.0.7 contain a vulnerability in some configurations. An attacker may exploit this vulnerability to gain access to restricted files. The non-RAN HTTP and WebDAV file-serving components have a vulnerability	N/A	A-DEL-EMC_-180220/52

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			wherein when either are enabled, and Basic Authentication is enabled for either or both components, files are accessible without authentication. **CVE ID : CVE-2020-5318**		
emc_unity_xt_operating_environment					
Improper Validation of Array Index	06-02-2020	7.8	Dell EMC Unity, Dell EMC Unity XT, and Dell EMC UnityVSA versions prior to 5.0.2.0.5.009 contain a Denial of Service vulnerability on NAS Server SSH implementation that is used to provide SFTP service on a NAS server. A remote unauthenticated attacker may potentially exploit this vulnerability and cause a Denial of Service (Storage Processor Panic) by sending an out of order SSH protocol sequence. **CVE ID : CVE-2020-5319**	N/A	A-DEL-EMC_-180220/53
Djangoproject					
django					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-02-2020	7.5	Django 1.11 before 1.11.28, 2.2 before 2.2.10, and 3.0 before 3.0.3 allows SQL Injection if untrusted data is used as a StringAgg delimiter (e.g., in Django applications that offer downloads of data as a series of rows with a user-	https://docs.djangoproject.com/en/3.0/releases/security/, https://github.com/django/django/commit/eb31d	A-DJA-DJAN-180220/54

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specified column delimiter). By passing a suitably crafted delimiter to a contrib.postgres.aggregates.StringAgg instance, it was possible to break escaping and inject malicious SQL. **CVE ID : CVE-2020-7471**	845323618d688ad429479c6dda973056136, https://groups.google.com/forum/#!topic/django-announce/X45S86X5bZI	
Dotcms					
dotcms					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-02-2020	7.5	dotCMS before 5.2.4 is vulnerable to directory traversal, leading to incorrect access control. It allows an attacker to read or execute files under $TOMCAT_HOME/webapps/ROOT/assets (which should be a protected directory). Additionally, attackers can upload temporary files (e.g., .jsp files) into /webapps/ROOT/assets/tmp_upload, which can lead to remote command execution (with the permissions of the user running the dotCMS application). **CVE ID : CVE-2020-6754**	https://dotcms.com/security/SI-54, https://github.com/dotCMS/core/issues/17796	A-DOT-DOTC-180220/55
dot-prop_project					
dot-prop					
Direct Request ('Forced Browsing')	04-02-2020	7.5	Prototype pollution vulnerability in dot-prop npm package version 5.1.0 and earlier allows an	N/A	A-DOT-DOT--180220/56

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to add arbitrary properties to JavaScript language constructs such as objects. **CVE ID : CVE-2020-8116**		
eginnovations					
eg_manager					
Improper Authentication	03-02-2020	7.5	eG Manager 7.1.2 allows authentication bypass via a com.egurkha.EgLoginServlet?uname=admin&upass=&accessKey=eGm0n1t0r request. **CVE ID : CVE-2020-8591**	N/A	A-EGI-EG_M-180220/57
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-02-2020	7.5	eG Manager 7.1.2 allows SQL Injection via the user parameter to com.eg.LoginHelperServlet (aka the Forgot Password feature). **CVE ID : CVE-2020-8592**	N/A	A-EGI-EG_M-180220/58
Eyesofnetwork					
eyesofnetwork					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-02-2020	9	An issue was discovered in EyesOfNetwork 5.3. An authenticated web user with sufficient privileges could abuse the AutoDiscovery module to run arbitrary OS commands via the /module/module_frame/index.php autodiscovery.php target field.	N/A	A-EYE-EYES-180220/59

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8654		
Improper Privilege Management	07-02-2020	9.3	An issue was discovered in EyesOfNetwork 5.3. The sudoers configuration is prone to a privilege escalation vulnerability, allowing the apache user to run arbitrary commands as root via a crafted NSE script for nmap 7. **CVE ID : CVE-2020-8655**	N/A	A-EYE-EYES-180220/60
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-02-2020	7.5	An issue was discovered in EyesOfNetwork 5.3. The EyesOfNetwork API 2.4.2 is prone to SQL injection, allowing an unauthenticated attacker to perform various tasks such as authentication bypass via the username field to getApiKey in include/api_functions.php. **CVE ID : CVE-2020-8656**	N/A	A-EYE-EYES-180220/61
Insufficiently Protected Credentials	06-02-2020	5	An issue was discovered in EyesOfNetwork 5.3. The installation uses the same API key (hardcoded as EONAPI_KEY in include/api_functions.php for API version 2.4.2) by default for all installations, hence allowing an attacker to calculate/guess the admin access token. **CVE ID : CVE-2020-8657**	N/A	A-EYE-EYES-180220/62
F5					
traffix_sdc					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-02-2020	4.3	On BIG-IP 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.6.0-11.6.5.1, the tmm crashes under certain circumstances when using the connector profile if a specific sequence of connections are made. **CVE ID : CVE-2020-5854**	https://support.f5.com/csp/article/K50046200	A-F5-TRAF-180220/63
big-ip_access_policy_manager					
Improper Input Validation	06-02-2020	4.3	On BIG-IP 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.6.0-11.6.5.1, the tmm crashes under certain circumstances when using the connector profile if a specific sequence of connections are made. **CVE ID : CVE-2020-5854**	https://support.f5.com/csp/article/K50046200	A-F5-BIG--180220/64
Incorrect Authorization	06-02-2020	4.6	When the Windows Logon Integration feature is configured for all versions of BIG-IP Edge Client for Windows, unauthorized users who have physical access to an authorized user's machine can get shell access under unprivileged user. **CVE ID : CVE-2020-5855**	https://support.f5.com/csp/article/K55102004	A-F5-BIG--180220/65
Improper Input Validation	06-02-2020	5	On BIG-IP 15.0.0-15.0.1.1 and 14.1.0-14.1.2.2, while processing specifically crafted traffic using the default 'xnet' driver,	https://support.f5.com/csp/article/K00025388	A-F5-BIG--180220/66

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Virtual Edition instances hosted in Amazon Web Services (AWS) may experience a TMM restart. **CVE ID : CVE-2020-5856**		
big-ip_advanced_firewall_manager					
Improper Input Validation	06-02-2020	4.3	On BIG-IP 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.6.0-11.6.5.1, the tmm crashes under certain circumstances when using the connector profile if a specific sequence of connections are made. **CVE ID : CVE-2020-5854**	https://support.f5.com/csp/article/K50046200	A-F5-BIG--180220/67
Improper Input Validation	06-02-2020	5	On BIG-IP 15.0.0-15.0.1.1 and 14.1.0-14.1.2.2, while processing specifically crafted traffic using the default 'xnet' driver, Virtual Edition instances hosted in Amazon Web Services (AWS) may experience a TMM restart. **CVE ID : CVE-2020-5856**	https://support.f5.com/csp/article/K00025388	A-F5-BIG--180220/68
big-ip_analytics					
Improper Input Validation	06-02-2020	4.3	On BIG-IP 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.6.0-11.6.5.1, the tmm crashes under certain circumstances when using the connector profile if a specific sequence of connections are made.	https://support.f5.com/csp/article/K50046200	A-F5-BIG--180220/69

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5854		
Improper Input Validation	06-02-2020	5	On BIG-IP 15.0.0-15.0.1.1 and 14.1.0-14.1.2.2, while processing specifically crafted traffic using the default 'xnet' driver, Virtual Edition instances hosted in Amazon Web Services (AWS) may experience a TMM restart. **CVE ID : CVE-2020-5856**	https://support.f5.com/csp/article/K00025388	A-F5-BIG--180220/70
big-ip_application_acceleration_manager					
Improper Input Validation	06-02-2020	4.3	On BIG-IP 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.6.0-11.6.5.1, the tmm crashes under certain circumstances when using the connector profile if a specific sequence of connections are made. **CVE ID : CVE-2020-5854**	https://support.f5.com/csp/article/K50046200	A-F5-BIG--180220/71
Improper Input Validation	06-02-2020	5	On BIG-IP 15.0.0-15.0.1.1 and 14.1.0-14.1.2.2, while processing specifically crafted traffic using the default 'xnet' driver, Virtual Edition instances hosted in Amazon Web Services (AWS) may experience a TMM restart. **CVE ID : CVE-2020-5856**	https://support.f5.com/csp/article/K00025388	A-F5-BIG--180220/72
big-ip_application_security_manager					
Improper Input Validation	06-02-2020	4.3	On BIG-IP 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.6.0-	https://support.f5.com/csp/article/K50046200	A-F5-BIG--180220/73

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			11.6.5.1, the tmm crashes under certain circumstances when using the connector profile if a specific sequence of connections are made. **CVE ID : CVE-2020-5854**		
Improper Input Validation	06-02-2020	5	On BIG-IP 15.0.0-15.0.1.1 and 14.1.0-14.1.2.2, while processing specifically crafted traffic using the default 'xnet' driver, Virtual Edition instances hosted in Amazon Web Services (AWS) may experience a TMM restart. **CVE ID : CVE-2020-5856**	https://support.f5.com/csp/article/K00025388	A-F5-BIG--180220/74
big-ip_domain_name_system					
Improper Input Validation	06-02-2020	4.3	On BIG-IP 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.6.0-11.6.5.1, the tmm crashes under certain circumstances when using the connector profile if a specific sequence of connections are made. **CVE ID : CVE-2020-5854**	https://support.f5.com/csp/article/K50046200	A-F5-BIG--180220/75
Improper Input Validation	06-02-2020	5	On BIG-IP 15.0.0-15.0.1.1 and 14.1.0-14.1.2.2, while processing specifically crafted traffic using the default 'xnet' driver, Virtual Edition instances hosted in Amazon Web Services (AWS) may experience a TMM restart.	https://support.f5.com/csp/article/K00025388	A-F5-BIG--180220/76

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5856		
big-ip_edge_gateway					
Improper Input Validation	06-02-2020	4.3	On BIG-IP 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.6.0-11.6.5.1, the tmm crashes under certain circumstances when using the connector profile if a specific sequence of connections are made. **CVE ID : CVE-2020-5854**	https://support.f5.com/csp/article/K50046200	A-F5-BIG--180220/77
big-ip_fraud_protection_service					
Improper Input Validation	06-02-2020	4.3	On BIG-IP 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.6.0-11.6.5.1, the tmm crashes under certain circumstances when using the connector profile if a specific sequence of connections are made. **CVE ID : CVE-2020-5854**	https://support.f5.com/csp/article/K50046200	A-F5-BIG--180220/78
Improper Input Validation	06-02-2020	5	On BIG-IP 15.0.0-15.0.1.1 and 14.1.0-14.1.2.2, while processing specifically crafted traffic using the default 'xnet' driver, Virtual Edition instances hosted in Amazon Web Services (AWS) may experience a TMM restart. **CVE ID : CVE-2020-5856**	https://support.f5.com/csp/article/K00025388	A-F5-BIG--180220/79
big-ip_global_traffic_manager					
Improper Input	06-02-2020	4.3	On BIG-IP 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-	https://support.f5.com/cs	A-F5-BIG--180220/80

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.6.0-11.6.5.1, the tmm crashes under certain circumstances when using the connector profile if a specific sequence of connections are made. **CVE ID : CVE-2020-5854**	p/article/K50046200	
Improper Input Validation	06-02-2020	5	On BIG-IP 15.0.0-15.0.1.1 and 14.1.0-14.1.2.2, while processing specifically crafted traffic using the default 'xnet' driver, Virtual Edition instances hosted in Amazon Web Services (AWS) may experience a TMM restart. **CVE ID : CVE-2020-5856**	https://support.f5.com/csp/article/K00025388	A-F5-BIG--180220/81
big-ip_link_controller					
Improper Input Validation	06-02-2020	4.3	On BIG-IP 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.6.0-11.6.5.1, the tmm crashes under certain circumstances when using the connector profile if a specific sequence of connections are made. **CVE ID : CVE-2020-5854**	https://support.f5.com/csp/article/K50046200	A-F5-BIG--180220/82
Improper Input Validation	06-02-2020	5	On BIG-IP 15.0.0-15.0.1.1 and 14.1.0-14.1.2.2, while processing specifically crafted traffic using the default 'xnet' driver, Virtual Edition instances hosted in Amazon Web Services (AWS) may	https://support.f5.com/csp/article/K00025388	A-F5-BIG--180220/83

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			experience a TMM restart. **CVE ID : CVE-2020-5856**		
big-ip_local_traffic_manager					
Improper Input Validation	06-02-2020	4.3	On BIG-IP 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.6.0-11.6.5.1, the tmm crashes under certain circumstances when using the connector profile if a specific sequence of connections are made. **CVE ID : CVE-2020-5854**	https://support.f5.com/csp/article/K50046200	A-F5-BIG--180220/84
Improper Input Validation	06-02-2020	5	On BIG-IP 15.0.0-15.0.1.1 and 14.1.0-14.1.2.2, while processing specifically crafted traffic using the default 'xnet' driver, Virtual Edition instances hosted in Amazon Web Services (AWS) may experience a TMM restart. **CVE ID : CVE-2020-5856**	https://support.f5.com/csp/article/K00025388	A-F5-BIG--180220/85
big-ip_policy_enforcement_manager					
Improper Input Validation	06-02-2020	4.3	On BIG-IP 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.6.0-11.6.5.1, the tmm crashes under certain circumstances when using the connector profile if a specific sequence of connections are made. **CVE ID : CVE-2020-5854**	https://support.f5.com/csp/article/K50046200	A-F5-BIG--180220/86
Improper Input	06-02-2020	5	On BIG-IP 15.0.0-15.0.1.1 and 14.1.0-14.1.2.2, while	https://support.f5.com/cs	A-F5-BIG--180220/87

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			processing specifically crafted traffic using the default 'xnet' driver, Virtual Edition instances hosted in Amazon Web Services (AWS) may experience a TMM restart. **CVE ID : CVE-2020-5856**	p/article/K00025388	
big-ip_webaccelerator					
Improper Input Validation	06-02-2020	4.3	On BIG-IP 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.6.0-11.6.5.1, the tmm crashes under certain circumstances when using the connector profile if a specific sequence of connections are made. **CVE ID : CVE-2020-5854**	https://support.f5.com/csp/article/K50046200	A-F5-BIG--180220/88
enterprise_manager					
Improper Input Validation	06-02-2020	4.3	On BIG-IP 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.6.0-11.6.5.1, the tmm crashes under certain circumstances when using the connector profile if a specific sequence of connections are made. **CVE ID : CVE-2020-5854**	https://support.f5.com/csp/article/K50046200	A-F5-ENTE-180220/89
big-iq_centralized_management					
Improper Input Validation	06-02-2020	4.3	On BIG-IP 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.6.0-11.6.5.1, the tmm crashes	https://support.f5.com/csp/article/K50046200	A-F5-BIG--180220/90

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			under certain circumstances when using the connector profile if a specific sequence of connections are made. **CVE ID : CVE-2020-5854**		
iworkflow					
Improper Input Validation	06-02-2020	4.3	On BIG-IP 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.6.0-11.6.5.1, the tmm crashes under certain circumstances when using the connector profile if a specific sequence of connections are made. **CVE ID : CVE-2020-5854**	https://support.f5.com/csp/article/K50046200	A-F5-IWOR-180220/91
big-ip_access_policy_manager_client					
Incorrect Authorization	06-02-2020	4.6	When the Windows Logon Integration feature is configured for all versions of BIG-IP Edge Client for Windows, unauthorized users who have physical access to an authorized user's machine can get shell access under unprivileged user. **CVE ID : CVE-2020-5855**	https://support.f5.com/csp/article/K55102004	A-F5-BIG--180220/92
Gitlab					
gitlab					
Information Exposure	05-02-2020	5	An issue was discovered in GitLab EE 11.3 and later. A GitLab Workhorse bypass could lead to package and file disclosure via request smuggling.	https://about.gitlab.com/releases/2020/01/30/security-release-	A-GIT-GITL-180220/93

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-6833	gitlab-12-7-4-released/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-02-2020	5	GitLab EE 11.11 and later through 12.7.2 allows Directory Traversal. **CVE ID : CVE-2020-7966**	https://about.gitlab.com/releases/2020/01/30/security-release-gitlab-12-7-4-released/	A-GIT-GITL-180220/94
Incorrect Default Permissions	05-02-2020	4	GitLab EE 8.0 through 12.7.2 has Insecure Permissions (issue 1 of 2). **CVE ID : CVE-2020-7967**	https://about.gitlab.com/releases/2020/01/30/security-release-gitlab-12-7-4-released/	A-GIT-GITL-180220/95
Improper Authentication	05-02-2020	5	GitLab EE 8.0 through 12.7.2 has Incorrect Access Control. **CVE ID : CVE-2020-7968**	https://about.gitlab.com/releases/2020/01/30/security-release-gitlab-12-7-4-released/	A-GIT-GITL-180220/96
Information Exposure	05-02-2020	5	GitLab EE 8.0 and later through 12.7.2 allows Information Disclosure. **CVE ID : CVE-2020-7969**	https://about.gitlab.com/releases/2020/01/30/security-release-gitlab-12-7-4-released/	A-GIT-GITL-180220/97
Improper Neutralization of Input During Web Page Generation	05-02-2020	4.3	GitLab EE 11.0 and later through 12.7.2 allows XSS. **CVE ID : CVE-2020-7971**	https://about.gitlab.com/releases/2020/01/30/security-release-	A-GIT-GITL-180220/98

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')				gitlab-12-7-4-released/	
Incorrect Default Permissions	05-02-2020	5	GitLab EE 12.2 has Insecure Permissions (issue 2 of 2). **CVE ID : CVE-2020-7972**	https://about.gitlab.com/releases/2020/01/30/security-release-gitlab-12-7-4-released/	A-GIT-GITL-180220/99
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-02-2020	4.3	GitLab through 12.7.2 allows XSS. **CVE ID : CVE-2020-7973**	https://about.gitlab.com/releases/2020/01/30/security-release-gitlab-12-7-4-released/	A-GIT-GITL-180220/100
Information Exposure	05-02-2020	5	GitLab EE 10.1 through 12.7.2 allows Information Disclosure. **CVE ID : CVE-2020-7974**	https://about.gitlab.com/releases/2020/01/30/security-release-gitlab-12-7-4-released/	A-GIT-GITL-180220/101
Information Exposure	05-02-2020	5	GitLab EE 12.4 and later through 12.7.2 has Incorrect Access Control. **CVE ID : CVE-2020-7976**	https://about.gitlab.com/releases/2020/01/30/security-release-gitlab-12-7-4-released/	A-GIT-GITL-180220/102
Incorrect Default Permissions	05-02-2020	4.3	GitLab EE 8.8 and later through 12.7.2 has Insecure Permissions. **CVE ID : CVE-2020-7977**	https://about.gitlab.com/releases/2020/01/30/security-release-	A-GIT-GITL-180220/103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				gitlab-12-7-4-released/	
N/A	05-02-2020	5	GitLab EE 12.6 and later through 12.7.2 allows Denial of Service. **CVE ID : CVE-2020-7978**	https://about.gitlab.com/releases/2020/01/30/security-release-gitlab-12-7-4-released/	A-GIT-GITL-180220/104
Incorrect Default Permissions	05-02-2020	4.3	GitLab EE 8.9 and later through 12.7.2 has Insecure Permission **CVE ID : CVE-2020-7979**	https://about.gitlab.com/releases/2020/01/30/security-release-gitlab-12-7-4-released/	A-GIT-GITL-180220/105
Incorrect Default Permissions	05-02-2020	7.5	GitLab EE 8.9 and later through 12.7.2 has Insecure Permission **CVE ID : CVE-2020-8114**	https://about.gitlab.com/releases/2020/01/30/security-release-gitlab-12-7-4-released/	A-GIT-GITL-180220/106
Google					
chrome					
Use After Free	11-02-2020	6.8	Use after free in speech in Google Chrome prior to 79.0.3945.130 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6378**	N/A	A-GOO-CHRO-180220/107
Use After Free	11-02-2020	6.8	Use after free in V8 in Google Chrome prior to 79.0.3945.130 allowed a	N/A	A-GOO-CHRO-180220/108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6379**		
Improper Input Validation	11-02-2020	6.8	Insufficient policy enforcement in extensions in Google Chrome prior to 79.0.3945.130 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted Chrome Extension. **CVE ID : CVE-2020-6380**	N/A	A-GOO-CHRO-180220/109
Integer Overflow or Wraparound	11-02-2020	6.8	Integer overflow in JavaScript in Google Chrome on ChromeOS and Android prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6381**	N/A	A-GOO-CHRO-180220/110
Access of Resource Using Incompatible Type ('Type Confusion')	11-02-2020	6.8	Type confusion in JavaScript in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6382**	N/A	A-GOO-CHRO-180220/111
Improper Input Validation	11-02-2020	6.8	Insufficient policy enforcement in storage in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass	N/A	A-GOO-CHRO-180220/112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			site isolation via a crafted HTML page. **CVE ID : CVE-2020-6385**		
Out-of-bounds Write	11-02-2020	6.8	Out of bounds write in WebRTC in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted video stream. **CVE ID : CVE-2020-6387**	N/A	A-GOO-CHRO-180220/113
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	6.8	Out of bounds access in WebAudio in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6388**	N/A	A-GOO-CHRO-180220/114
Out-of-bounds Write	11-02-2020	6.8	Out of bounds write in WebRTC in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted video stream. **CVE ID : CVE-2020-6389**	N/A	A-GOO-CHRO-180220/115
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	6.8	Out of bounds memory access in streams in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6390**	N/A	A-GOO-CHRO-180220/116
Improper	11-02-2020	4.3	Insufficient validation of	N/A	A-GOO-CHRO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			untrusted input in Blink in Google Chrome prior to 80.0.3987.87 allowed a local attacker to bypass content security policy via a crafted HTML page. **CVE ID : CVE-2020-6391**		180220/117
Improper Input Validation	11-02-2020	4.3	Insufficient policy enforcement in extensions in Google Chrome prior to 80.0.3987.87 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension. **CVE ID : CVE-2020-6392**	N/A	A-GOO-CHRO-180220/118
Improper Input Validation	11-02-2020	4.3	Insufficient policy enforcement in Blink in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to leak cross-origin data via a crafted HTML page. **CVE ID : CVE-2020-6393**	N/A	A-GOO-CHRO-180220/119
Improper Input Validation	11-02-2020	5.8	Insufficient policy enforcement in Blink in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass content security policy via a crafted HTML page. **CVE ID : CVE-2020-6394**	N/A	A-GOO-CHRO-180220/120
Out-of-bounds Read	11-02-2020	4.3	Out of bounds read in JavaScript in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to obtain	N/A	A-GOO-CHRO-180220/121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially sensitive information from process memory via a crafted HTML page. **CVE ID : CVE-2020-6395**		
Improper Input Validation	11-02-2020	4.3	Inappropriate implementation in Skia in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. **CVE ID : CVE-2020-6396**	N/A	A-GOO-CHRO-180220/122
Improper Input Validation	11-02-2020	4.3	Inappropriate implementation in sharing in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to spoof security UI via a crafted HTML page. **CVE ID : CVE-2020-6397**	N/A	A-GOO-CHRO-180220/123
N/A	11-02-2020	6.8	Use of uninitialized data in PDFium in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. **CVE ID : CVE-2020-6398**	N/A	A-GOO-CHRO-180220/124
Improper Input Validation	11-02-2020	4.3	Insufficient policy enforcement in AppCache in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to leak cross-origin data via a crafted HTML page. **CVE ID : CVE-2020-6399**	N/A	A-GOO-CHRO-180220/125

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	11-02-2020	4.3	Inappropriate implementation in CORS in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to leak cross-origin data via a crafted HTML page. **CVE ID : CVE-2020-6400**	N/A	A-GOO-CHRO-180220/126
Improper Input Validation	11-02-2020	4.3	Insufficient validation of untrusted input in Omnibox in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name. **CVE ID : CVE-2020-6401**	N/A	A-GOO-CHRO-180220/127
Improper Input Validation	11-02-2020	6.8	Insufficient policy enforcement in downloads in Google Chrome on OS X prior to 80.0.3987.87 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted Chrome Extension. **CVE ID : CVE-2020-6402**	N/A	A-GOO-CHRO-180220/128
Improper Input Validation	11-02-2020	4.3	Incorrect implementation in Omnibox in Google Chrome on iOS prior to 80.0.3987.87 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. **CVE ID : CVE-2020-6403**	N/A	A-GOO-CHRO-180220/129

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	4.6	Inappropriate implementation in Blink in Google Chrome prior to 80.0.3987.87 allowed a local attacker to potentially exploit heap corruption via crafted clipboard content. **CVE ID : CVE-2020-6404**	N/A	A-GOO-CHRO-180220/130
Out-of-bounds Read	11-02-2020	4.3	Out of bounds read in SQLite in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. **CVE ID : CVE-2020-6405**	N/A	A-GOO-CHRO-180220/131
Use After Free	11-02-2020	9.3	Use after free in audio in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6406**	N/A	A-GOO-CHRO-180220/132
Information Exposure	11-02-2020	2.1	Insufficient policy enforcement in CORS in Google Chrome prior to 80.0.3987.87 allowed a local attacker to obtain potentially sensitive information via a crafted HTML page. **CVE ID : CVE-2020-6408**	N/A	A-GOO-CHRO-180220/133
N/A	11-02-2020	6.8	Inappropriate implementation in Omnibox in Google Chrome prior to	N/A	A-GOO-CHRO-180220/134

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			80.0.3987.87 allowed a remote attacker who convinced the user to enter a URI to bypass navigation restrictions via a crafted domain name. **CVE ID : CVE-2020-6409**		
N/A	11-02-2020	6.8	Insufficient policy enforcement in navigation in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to confuse the user via a crafted domain name. **CVE ID : CVE-2020-6410**	N/A	A-GOO-CHRO-180220/135
Improper Input Validation	11-02-2020	5.8	Insufficient validation of untrusted input in Omnibox in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name. **CVE ID : CVE-2020-6411**	N/A	A-GOO-CHRO-180220/136
Improper Input Validation	11-02-2020	5.8	Insufficient validation of untrusted input in Omnibox in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name. **CVE ID : CVE-2020-6412**	N/A	A-GOO-CHRO-180220/137
N/A	11-02-2020	6.8	Inappropriate implementation in Blink in Google Chrome prior to 80.0.3987.87 allowed a	N/A	A-GOO-CHRO-180220/138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to bypass HTML validators via a crafted HTML page. **CVE ID : CVE-2020-6413**		
N/A	11-02-2020	6.8	Insufficient policy enforcement in Safe Browsing in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. **CVE ID : CVE-2020-6414**	N/A	A-GOO-CHRO-180220/139
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	6.8	Inappropriate implementation in JavaScript in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6415**	N/A	A-GOO-CHRO-180220/140
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	6.8	Insufficient data validation in streams in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6416**	N/A	A-GOO-CHRO-180220/141
N/A	11-02-2020	4.6	Inappropriate implementation in installer in Google Chrome prior to 80.0.3987.87 allowed a local attacker to execute arbitrary code via	N/A	A-GOO-CHRO-180220/142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a crafted registry entry. **CVE ID : CVE-2020-6417**		
htmlunit_project					
htmlunit					
Improper Initialization	11-02-2020	6.8	HtmlUnit prior to 2.37.0 contains code execution vulnerabilities. HtmlUnit initializes Rhino engine improperly, hence a malicious JavScript code can execute arbitrary Java code on the application. Moreover, when embedded in Android application, Android-specific initialization of Rhino engine is done in an improper way, hence a malicious JavaScript code can execute arbitrary Java code on the application. **CVE ID : CVE-2020-5529**	https://github.com/HtmlUnit/htmlunit/releases/tag/2.37.0	A-HTM-HTML-180220/143
IBM					
storediq					
Information Exposure	03-02-2020	2.1	IBM StoredIQ 7.6.0.17 through 7.6.0.20 could disclose sensitive information to a local user due to data in certain directories not being encrypted when it contained symbolic links. IBM X-Force ID: 175133. **CVE ID : CVE-2020-4224**	https://www.ibm.com/support/pages/node/1288150	A-IBM-STOR-180220/144
websphere_application_server					
Improper Privilege	04-02-2020	6	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0, under	https://www.ibm.com/support/page	A-IBM-WEBS-180220/145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			specialized conditions, could allow an authenticated user to create a maliciously crafted file name which would be misinterpreted as jsp content and executed. IBM X-Force ID: 174397. **CVE ID : CVE-2020-4163**	s/node/1288786	
Icewarp					
icewarp_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-02-2020	4.3	In IceWarp Webmail Server through 11.4.4.1, there is XSS in the /webmail/ color parameter. **CVE ID : CVE-2020-8512**	N/A	A-ICE-ICEW-180220/146
ipmitool_project					
ipmitool					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	05-02-2020	6.5	It's been found that multiple functions in ipmitool before 1.8.19 neglect proper checking of the data received from a remote LAN party, which may lead to buffer overflows and potentially to remote code execution on the ipmitool side. This is especially dangerous if ipmitool is run as a privileged user. This problem is fixed in version 1.8.19. **CVE ID : CVE-2020-5208**	https://github.com/ipmitool/ipmitool/security/advisories/GHSA-g659-9qxw-p7cp	A-IPM-IPMI-180220/147

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
istio					
istio					
Improper Authentication	12-02-2020	7.5	Istio 1.3 through 1.4.3 allows authentication bypass. The Authentication Policy exact-path matching logic can allow unauthorized access to HTTP paths even if they are configured to be only accessed after presenting a valid JWT token. For example, an attacker can add a ? or # character to a URI that would otherwise satisfy an exact-path match. **CVE ID : CVE-2020-8595**	https://access.redhat.com/security/cve/cve-2020-8595, https://istio.io/news/security/istio-security-2020-001/	A-IST-ISTI-180220/148
Jenkins					
google_kubernetes_engine					
N/A	12-02-2020	6.5	Jenkins Google Kubernetes Engine Plugin 0.8.0 and earlier does not configure its YAML parser to prevent the instantiation of arbitrary types, resulting in a remote code execution vulnerability. **CVE ID : CVE-2020-2121**	https://jenkins.io/security/advisory/2020-02-12/#SECURITY-1731	A-JEN-GOOG-180220/149
script_security					
Improper Input Validation	12-02-2020	6.5	Sandbox protection in Jenkins Script Security Plugin 1.69 and earlier could be circumvented during the script compilation phase by applying AST transforming annotations to imports or	https://jenkins.io/security/advisory/2020-02-12/#SECURITY-1713	A-JEN-SCRI-180220/150

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			by using them inside of other annotations. **CVE ID : CVE-2020-2110**		
pipeline					
Improper Input Validation	12-02-2020	6.5	Sandbox protection in Jenkins Pipeline: Groovy Plugin 2.78 and earlier can be circumvented through default parameter expressions in CPS-transformed methods. **CVE ID : CVE-2020-2109**	https://jenkins.io/security/advisory/2020-02-12/#SECURITY-1710	A-JEN-PIPE-180220/151
subversion					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-02-2020	3.5	Jenkins Subversion Plugin 2.13.0 and earlier does not escape the error message for the Project Repository Base URL field form validation, resulting in a stored cross-site scripting vulnerability. **CVE ID : CVE-2020-2111**	https://jenkins.io/security/advisory/2020-02-12/#SECURITY-1725	A-JEN-SUBV-180220/152
git_parameter					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-02-2020	3.5	Jenkins Git Parameter Plugin 0.9.11 and earlier does not escape the parameter name shown on the UI, resulting in a stored cross-site scripting vulnerability exploitable by users with Job/Configure permission. **CVE ID : CVE-2020-2112**	https://jenkins.io/security/advisory/2020-02-12/#SECURITY-1709	A-JEN-GIT_-180220/153
Improper Neutralization of Input During Web Page	12-02-2020	3.5	Jenkins Git Parameter Plugin 0.9.11 and earlier does not escape the default value shown on the UI, resulting in a stored cross-	https://jenkins.io/security/advisory/2020-02-12/#SECURI	A-JEN-GIT_-180220/154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			site scripting vulnerability exploitable by users with Job/Configure permission. **CVE ID : CVE-2020-2113**	TY-1709	
s3_publisher					
Insufficiently Protected Credentials	12-02-2020	5	Jenkins S3 publisher Plugin 0.11.4 and earlier transmits configured credentials in plain text as part of the global Jenkins configuration form, potentially resulting in their exposure. **CVE ID : CVE-2020-2114**	https://jenkins.io/security/advisory/2020-02-12/#SECURITY-1684	A-JEN-S3_P-180220/155
nunit					
Improper Restriction of XML External Entity Reference ('XXE')	12-02-2020	6.5	Jenkins NUnit Plugin 0.25 and earlier does not configure the XML parser to prevent XML external entity (XXE) attacks. **CVE ID : CVE-2020-2115**	https://jenkins.io/security/advisory/2020-02-12/#SECURITY-1752	A-JEN-NUNI-180220/156
pipeline_github_notify_step					
Cross-Site Request Forgery (CSRF)	12-02-2020	6.8	A cross-site request forgery vulnerability in Jenkins Pipeline GitHub Notify Step Plugin 1.0.4 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. **CVE ID : CVE-2020-2116**	https://jenkins.io/security/advisory/2020-02-12/#SECURITY-812%20(1)	A-JEN-PIPE-180220/157
Incorrect Default	12-02-2020	4	A missing permission check in Jenkins Pipeline	https://jenkins.io/securit	A-JEN-PIPE-180220/158

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Permissions			GitHub Notify Step Plugin 1.0.4 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. **CVE ID : CVE-2020-2117**	y/advisory/2020-02-12/#SECURITY-812%20(1)	
Incorrect Default Permissions	12-02-2020	4	A missing permission check in Jenkins Pipeline GitHub Notify Step Plugin 1.0.4 and earlier in form-related methods allowed users with Overall/Read access to enumerate credentials ID of credentials stored in Jenkins. **CVE ID : CVE-2020-2118**	https://jenkins.io/security/advisory/2020-02-12/#SECURITY-812%20(2)	A-JEN-PIPE-180220/159
fitnesse					
Improper Restriction of XML External Entity Reference ('XXE')	12-02-2020	6.5	Jenkins FitNesse Plugin 1.30 and earlier does not configure the XML parser to prevent XML external entity (XXE) attacks. **CVE ID : CVE-2020-2120**	https://jenkins.io/security/advisory/2020-02-12/#SECURITY-1751	A-JEN-FITN-180220/160
brakeman					
Improper Neutralization of Input During Web Page Generation ('Cross-site	12-02-2020	3.5	Jenkins Brakeman Plugin 0.12 and earlier did not escape values received from parsed JSON files when rendering them, resulting in a stored cross-site scripting vulnerability	https://jenkins.io/security/advisory/2020-02-12/#SECURITY-1644	A-JEN-BRAK-180220/161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			exploitable by users able to control the Brakeman post-build step input data. **CVE ID : CVE-2020-2122**		
radargun					
Deserialization of Untrusted Data	12-02-2020	6.5	Jenkins RadarGun Plugin 1.7 and earlier does not configure its YAML parser to prevent the instantiation of arbitrary types, resulting in a remote code execution vulnerability. **CVE ID : CVE-2020-2123**	https://jenkins.io/security/advisory/2020-02-12/#SECURITY-1733	A-JEN-RADA-180220/162
dynamic_extended_choice_parameter					
Insufficiently Protected Credentials	12-02-2020	4	Jenkins Dynamic Extended Choice Parameter Plugin 1.0.1 and earlier stores a password unencrypted in job config.xml files on the Jenkins master where it can be viewed by users with Extended Read permission, or access to the master file system. **CVE ID : CVE-2020-2124**	https://jenkins.io/security/advisory/2020-02-12/#SECURITY-1560	A-JEN-DYNA-180220/163
debian_package_builder					
Insufficiently Protected Credentials	12-02-2020	4	Jenkins Debian Package Builder Plugin 1.6.11 and earlier stores a GPG passphrase unencrypted in its global configuration file on the Jenkins master where it can be viewed by users with access to the master file system. **CVE ID : CVE-2020-2125**	https://jenkins.io/security/advisory/2020-02-12/#SECURITY-1558	A-JEN-DEBI-180220/164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
digitalocean					
Insufficiently Protected Credentials	12-02-2020	4	Jenkins DigitalOcean Plugin 1.1 and earlier stores a token unencrypted in the global config.xml file on the Jenkins master where it can be viewed by users with access to the master file system. **CVE ID : CVE-2020-2126**	https://jenkins.io/security/advisory/2020-02-12/#SECURITY-1559	A-JEN-DIGI-180220/165
bmc_release_package_and_deployment					
Insufficiently Protected Credentials	12-02-2020	4	Jenkins BMC Release Package and Deployment Plugin 1.1 and earlier stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system. **CVE ID : CVE-2020-2127**	https://jenkins.io/security/advisory/2020-02-12/#SECURITY-1547	A-JEN-BMC_-180220/166
ecx_copy_data_management					
Insufficiently Protected Credentials	12-02-2020	4	Jenkins ECX Copy Data Management Plugin 1.9 and earlier stores a password unencrypted in job config.xml files on the Jenkins master where it can be viewed by users with Extended Read permission, or access to the master file system. **CVE ID : CVE-2020-2128**	https://jenkins.io/security/advisory/2020-02-12/#SECURITY-1549	A-JEN-ECX_-180220/167
eagle_tester					
Insufficiently Protected	12-02-2020	4	Jenkins Eagle Tester Plugin 1.0.9 and earlier stores a	https://jenkins.io/securit	A-JEN-EAGL-180220/168

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			password unencrypted in its global configuration file on the Jenkins master where it can be viewed by users with access to the master file system. **CVE ID : CVE-2020-2129**	y/advisory/2020-02-12/#SECURITY-1552	
harvest_scm					
Insufficiently Protected Credentials	12-02-2020	4	Jenkins Harvest SCM Plugin 0.5.1 and earlier stores a password unencrypted in its global configuration file on the Jenkins master where it can be viewed by users with access to the master file system. **CVE ID : CVE-2020-2130**	https://jenkins.io/security/advisory/2020-02-12/#SECURITY-1553	A-JEN-HARV-180220/169
Insufficiently Protected Credentials	12-02-2020	4	Jenkins Harvest SCM Plugin 0.5.1 and earlier stores passwords unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system. **CVE ID : CVE-2020-2131**	https://jenkins.io/security/advisory/2020-02-12/#SECURITY-1553	A-JEN-HARV-180220/170
parasoft_environment_manager					
Insufficiently Protected Credentials	12-02-2020	4	Jenkins Parasoft Environment Manager Plugin 2.14 and earlier stores a password unencrypted in job config.xml files on the Jenkins master where it can be viewed by users with Extended Read	https://jenkins.io/security/advisory/2020-02-12/#SECURITY-1562	A-JEN-PARA-180220/171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			permission, or access to the master file system. **CVE ID : CVE-2020-2132**		
applatix					
Insufficiently Protected Credentials	12-02-2020	4	Jenkins Applatix Plugin 1.1 and earlier stores a password unencrypted in job config.xml files on the Jenkins master where it can be viewed by users with Extended Read permission, or access to the master file system. **CVE ID : CVE-2020-2133**	https://jenkins.io/security/advisory/2020-02-12/#SECURITY-1540	A-JEN-APPL-180220/172
azure_ad					
Insufficiently Protected Credentials	12-02-2020	5	Jenkins Azure AD Plugin 1.1.2 and earlier transmits configured credentials in plain text as part of the global Jenkins configuration form, potentially resulting in their exposure. **CVE ID : CVE-2020-2119**	https://jenkins.io/security/advisory/2020-02-12/#SECURITY-1717	A-JEN-AZUR-180220/173
klona_project					
klona					
Improper Input Validation	04-02-2020	7.5	Flaw in input validation in npm package klona version 1.1.0 and earlier may allow prototype pollution attack that may result in remote code execution or denial of service of applications using klona. **CVE ID : CVE-2020-8125**	N/A	A-KLO-KLON-180220/174
libslirp_project					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
libslirp					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-02-2020	10	In libslirp 4.1.0, as used in QEMU 4.2.0, tcp_subr.c misuses snprintf return values, leading to a buffer overflow in later code. **CVE ID : CVE-2020-8608**	N/A	A-LIB-LIBS-180220/175
Linuxfoundation					
the_update_framework					
Improper Verification of Cryptographic Signature	05-02-2020	7.5	TUF (aka The Update Framework) through 0.12.1 has Improper Verification of a Cryptographic Signature. **CVE ID : CVE-2020-6174**	https://github.com/theupdateframework/tuf/pull/974	A-LIN-THE_-180220/176
lotus_core_cms_project					
lotus_core_cms					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-02-2020	6.5	Lotus Core CMS 1.0.1 allows authenticated Local File Inclusion of .php files via directory traversal in the index.php page_slug parameter. **CVE ID : CVE-2020-8641**	N/A	A-LOT-LOTU-180220/177
machothemes					
strong_testimonials					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-02-2020	4.3	Stored XSS in the Strong Testimonials plugin before 2.40.1 for WordPress can result in an attacker performing malicious actions such as stealing session tokens. **CVE ID : CVE-2020-8549**	N/A	A-MAC-STRO-180220/178
Mariadb					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mariadb					
Improper Privilege Management	04-02-2020	7.2	mysql_install_db in MariaDB 10.4.7 through 10.4.11 allows privilege escalation from the mysql user account to root because chown and chmod are performed unsafely, as demonstrated by a symlink attack on a chmod 04755 of auth_pam_tool_dir/auth_pam_tool. NOTE: this does not affect the Oracle MySQL product, which implements mysql_install_db differently. **CVE ID : CVE-2020-7221**	https://github.com/MariaDB/server/commit/9d18b6246755472c8324bf3e20e234e08ac45618	A-MAR-MARI-180220/179
masscode					
masscode					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-02-2020	4.3	massCode 1.0.0-alpha.6 allows XSS via crafted Markdown text, with resultant remote code execution (because nodeIntegration in webPreferences is true). **CVE ID : CVE-2020-8548**	N/A	A-MAS-MASS-180220/180
Maxum					
rumpus					
Improper Neutralization of Input During Web Page Generation ('Cross-site	02-02-2020	4.3	An issue was discovered in Rumpus 8.2.10 on macOS. By crafting a directory name, it is possible to activate JavaScript in the context of the web application after invoking	N/A	A-MAX-RUMP-180220/181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			the rename folder functionality. **CVE ID : CVE-2020-8514**		
Microsoft					
chakracore					
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767. **CVE ID : CVE-2020-0710**	N/A	A-MIC-CHAK-180220/182
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0710, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767. **CVE ID : CVE-2020-0711**	N/A	A-MIC-CHAK-180220/183
Improper Restriction of Operations within the Bounds of a	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory	N/A	A-MIC-CHAK-180220/184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0710, CVE-2020-0711, CVE-2020-0713, CVE-2020-0767. **CVE ID : CVE-2020-0712**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0767. **CVE ID : CVE-2020-0713**	N/A	A-MIC-CHAK-180220/185
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713. **CVE ID : CVE-2020-0767**	N/A	A-MIC-CHAK-180220/186
edge					
Improper Restriction	11-02-2020	7.6	A remote code execution vulnerability exists in the	N/A	A-MIC-EDGE-180220/187

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767. **CVE ID : CVE-2020-0710**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0710, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767. **CVE ID : CVE-2020-0711**	N/A	A-MIC-EDGE-180220/188
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0710, CVE-2020-0711, CVE-2020-0713, CVE-2020-0767.	N/A	A-MIC-EDGE-180220/189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0712		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0767. **CVE ID : CVE-2020-0713**	N/A	A-MIC-EDGE-180220/190
Improper Privilege Management	11-02-2020	4	An elevation of privilege vulnerability exists when Microsoft Edge does not properly enforce cross-domain policies, which could allow an attacker to access information from one domain and inject it into another domain.In a web-based attack scenario, an attacker could host a website that is used to attempt to exploit the vulnerability, aka 'Microsoft Edge Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0663**	N/A	A-MIC-EDGE-180220/191
Information Exposure	11-02-2020	4.3	An information disclosure vulnerability exists in the way that affected Microsoft browsers handle cross-origin requests, aka 'Microsoft Browser Information Disclosure	N/A	A-MIC-EDGE-180220/192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. **CVE ID : CVE-2020-0706**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713. **CVE ID : CVE-2020-0767**	N/A	A-MIC-EDGE-180220/193
office					
N/A	11-02-2020	4.3	A security feature bypass vulnerability exists in Microsoft Outlook software when it improperly handles the parsing of URI formats, aka 'Microsoft Outlook Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-0696**	N/A	A-MIC-OFFI-180220/194
office_365_proplus					
N/A	11-02-2020	4.3	A security feature bypass vulnerability exists in Microsoft Outlook software when it improperly handles the parsing of URI formats, aka 'Microsoft Outlook Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-0696**	N/A	A-MIC-OFFI-180220/195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Microsoft Office OLicenseHeartbeat task, where an attacker who successfully exploited this vulnerability could run this task as SYSTEM.To exploit the vulnerability, an authenticated attacker would need to place a specially crafted file in a specific location, thereby allowing arbitrary file corruption.The security update addresses the vulnerability by correcting how the process validates the log file., aka 'Microsoft Office Tampering Vulnerability'. **CVE ID : CVE-2020-0697**	N/A	A-MIC-OFFI-180220/196
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-0759**	N/A	A-MIC-OFFI-180220/197
internet_explorer					
Improper Restriction of Operations within the Bounds of a Memory	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'.	N/A	A-MIC-INTE-180220/198

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			This CVE ID is unique from CVE-2020-0674, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767. **CVE ID : CVE-2020-0673**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767. **CVE ID : CVE-2020-0674**	N/A	A-MIC-INTE-180220/199
Information Exposure	11-02-2020	4.3	An information disclosure vulnerability exists in the way that affected Microsoft browsers handle cross-origin requests, aka 'Microsoft Browser Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0706**	N/A	A-MIC-INTE-180220/200
outlook					
N/A	11-02-2020	4.3	A security feature bypass vulnerability exists in Microsoft Outlook software when it improperly handles the parsing of URI formats, aka 'Microsoft Outlook	N/A	A-MIC-OUTL-180220/201

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-0696**		
sharepoint_enterprise_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-02-2020	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-0694. **CVE ID : CVE-2020-0693**	N/A	A-MIC-SHAR-180220/202
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-02-2020	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-0693. **CVE ID : CVE-2020-0694**	N/A	A-MIC-SHAR-180220/203
exchange_server					
Deserialization of Untrusted Data	11-02-2020	9	A remote code execution vulnerability exists in Microsoft Exchange software when the software fails to properly handle objects in memory,	N/A	A-MIC-EXCH-180220/204

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			aka 'Microsoft Exchange Memory Corruption Vulnerability'. **CVE ID : CVE-2020-0688**		
Improper Privilege Management	11-02-2020	6.8	An elevation of privilege vulnerability exists in Microsoft Exchange Server, aka 'Microsoft Exchange Server Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0692**	N/A	A-MIC-EXCH-180220/205
excel					
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-0759**	N/A	A-MIC-EXCE-180220/206
sql_server					
Improper Input Validation	11-02-2020	6.5	A remote code execution vulnerability exists in Microsoft SQL Server Reporting Services when it incorrectly handles page requests, aka 'Microsoft SQL Server Reporting Services Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-0618**	N/A	A-MIC-SQL_-180220/207
windows_malicious_software_removal_tool					
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists when the Windows Malicious Software Removal Tool (MSRT) improperly	N/A	A-MIC-WIND-180220/208

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			handles junctions.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Malicious Software Removal Tool Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0733**		
minisnmpd_project					
minisnmpd					
Out-of-bounds Read	04-02-2020	6.4	An exploitable out-of-bounds read vulnerability exists in the way MiniSNMPD version 1.4 parses incoming SNMP packets. A specially crafted SNMP request can trigger an out-of-bounds memory read, which can result in the disclosure of sensitive information and denial of service. To trigger this vulnerability, an attacker needs to send a specially crafted packet to the vulnerable server. **CVE ID : CVE-2020-6058**	N/A	A-MIN-MINI-180220/209
Out-of-bounds Read	04-02-2020	6.4	An exploitable out of bounds read vulnerability exists in the way MiniSNMPD version 1.4 parses incoming SNMP packets. A specially crafted SNMP request can trigger an out of bounds memory read which can result in sensitive information	N/A	A-MIN-MINI-180220/210

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disclosure and Denial Of Service. In order to trigger this vulnerability, an attacker needs to send a specially crafted packet to the vulnerable server. **CVE ID : CVE-2020-6059**		
Out-of-bounds Write	04-02-2020	5	A stack buffer overflow vulnerability exists in the way MiniSNMPD version 1.4 handles multiple connections. A specially timed sequence of SNMP connections can trigger a stack overflow, resulting in a denial of service. To trigger this vulnerability, an attacker needs to simply initiate multiple connections to the server. **CVE ID : CVE-2020-6060**	N/A	A-MIN-MINI-180220/211
Misp					
misp					
Time-of-check Time-of-use (TOCTOU) Race Condition	12-02-2020	4.3	An issue was discovered in MISP before 2.4.121. It mishandled time skew (between the machine hosting the web server and the machine hosting the database) when trying to block a brute-force series of invalid requests. **CVE ID : CVE-2020-8890**	N/A	A-MIS-MISP-180220/212
N/A	12-02-2020	4.3	An issue was discovered in MISP before 2.4.121. It did not canonicalize usernames when trying to block a brute-force series	N/A	A-MIS-MISP-180220/213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of invalid requests. **CVE ID : CVE-2020-8891**		
N/A	12-02-2020	6.8	An issue was discovered in MISP before 2.4.121. It did not consider the HTTP PUT method when trying to block a brute-force series of invalid requests. **CVE ID : CVE-2020-8892**	N/A	A-MIS-MISP-180220/214
N/A	12-02-2020	5	An issue was discovered in MISP before 2.4.121. The Galaxy view contained an incorrectly sanitized search string in app/View/Galaxies/view.ctp. **CVE ID : CVE-2020-8893**	N/A	A-MIS-MISP-180220/215
N/A	12-02-2020	6.4	An issue was discovered in MISP before 2.4.121. ACLs for discussion threads were mishandled in app/Controller/ThreadsController.php and app/Model/Thread.php. **CVE ID : CVE-2020-8894**	N/A	A-MIS-MISP-180220/216
nanopb_project					
nanopb					
Out-of-bounds Read	04-02-2020	7.5	There is a potentially exploitable out of memory condition In Nanopb before 0.4.1, 0.3.9.5, and 0.2.9.4. When nanopb is compiled with PB_ENABLE_MALLOC, the message to be decoded contains a repeated string, bytes or message field and realloc() runs out of	https://github.com/nanopb/nanopb/security/advisories/GHSA-gcx3-7m76-287p	A-NAN-NANO-180220/217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory when expanding the array nanopb can end up calling `free()` on a pointer value that comes from uninitialized memory. Depending on platform this can result in a crash or further memory corruption, which may be exploitable in some cases. This problem is fixed in nanopb-0.4.1, nanopb-0.3.9.5, nanopb-0.2.9.4. **CVE ID : CVE-2020-5235**		
Nextcloud					
nextcloud_server					
Improper Preservation of Permissions	04-02-2020	4	Improper preservation of permissions in Nextcloud Server 14.0.3 causes the event details to be leaked when sharing a non-public event. **CVE ID : CVE-2020-8117**	N/A	A-NEX-NEXT-180220/218
Server-Side Request Forgery (SSRF)	04-02-2020	4	An authenticated server-side request forgery in Nextcloud server 16.0.1 allowed to detect local and remote services when adding a new subscription in the calendar application. **CVE ID : CVE-2020-8118**	N/A	A-NEX-NEXT-180220/219
Incorrect Authorization	04-02-2020	4	Improper authorization in Nextcloud server 17.0.0 causes leaking of previews and files when a file-drop share link is opened via the gallery app. **CVE ID : CVE-2020-8119**	N/A	A-NEX-NEXT-180220/220

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	04-02-2020	5.5	A bug in Nextcloud Server 14.0.4 could expose more data in reshared link shares than intended by the sharer. **CVE ID : CVE-2020-8121**	N/A	A-NEX-NEXT-180220/221
Improper Input Validation	04-02-2020	4	A missing check in Nextcloud Server 14.0.3 could give recipient the possibility to extend the expiration date of a share they received. **CVE ID : CVE-2020-8122**	N/A	A-NEX-NEXT-180220/222
nextcloud					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-02-2020	4.3	A reflected Cross-Site Scripting vulnerability in Nextcloud Server 16.0.1 was discovered in the svg generation. **CVE ID : CVE-2020-8120**	N/A	A-NEX-NEXT-180220/223
Norman					
malware_cleaner					
Out-of-bounds Write	03-02-2020	7.5	nsak64.sys in Norman Malware Cleaner 2.08.08 allows users to call arbitrary kernel functions because the passing of function pointers between user and kernel mode is mishandled. **CVE ID : CVE-2020-8508**	N/A	A-NOR-MALW-180220/224
Opensuse					
backports_sle					
Integer Overflow or	11-02-2020	6.8	Integer overflow in JavaScript in Google	N/A	A-OPE-BACK-180220/225

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			Chrome on ChromeOS and Android prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6381**		
Improper Input Validation	11-02-2020	6.8	Insufficient policy enforcement in storage in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass site isolation via a crafted HTML page. **CVE ID : CVE-2020-6385**	N/A	A-OPE-BACK-180220/226
Improper Input Validation	11-02-2020	4.3	Insufficient validation of untrusted input in Blink in Google Chrome prior to 80.0.3987.87 allowed a local attacker to bypass content security policy via a crafted HTML page. **CVE ID : CVE-2020-6391**	N/A	A-OPE-BACK-180220/227
Improper Input Validation	11-02-2020	4.3	Insufficient policy enforcement in extensions in Google Chrome prior to 80.0.3987.87 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension. **CVE ID : CVE-2020-6392**	N/A	A-OPE-BACK-180220/228
Improper Input Validation	11-02-2020	4.3	Insufficient policy enforcement in Blink in Google Chrome prior to 80.0.3987.87 allowed a	N/A	A-OPE-BACK-180220/229

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to leak cross-origin data via a crafted HTML page. **CVE ID : CVE-2020-6393**		
Improper Input Validation	11-02-2020	5.8	Insufficient policy enforcement in Blink in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass content security policy via a crafted HTML page. **CVE ID : CVE-2020-6394**	N/A	A-OPE-BACK-180220/230
Improper Input Validation	11-02-2020	4.3	Inappropriate implementation in Skia in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. **CVE ID : CVE-2020-6396**	N/A	A-OPE-BACK-180220/231
Improper Input Validation	11-02-2020	4.3	Inappropriate implementation in sharing in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to spoof security UI via a crafted HTML page. **CVE ID : CVE-2020-6397**	N/A	A-OPE-BACK-180220/232
N/A	11-02-2020	6.8	Use of uninitialized data in PDFium in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. **CVE ID : CVE-2020-6398**	N/A	A-OPE-BACK-180220/233
Improper	11-02-2020	4.3	Insufficient policy	N/A	A-OPE-BACK-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			enforcement in AppCache in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to leak cross-origin data via a crafted HTML page. **CVE ID : CVE-2020-6399**		180220/234
Information Exposure	11-02-2020	4.3	Inappropriate implementation in CORS in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to leak cross-origin data via a crafted HTML page. **CVE ID : CVE-2020-6400**	N/A	A-OPE-BACK-180220/235
Improper Input Validation	11-02-2020	4.3	Insufficient validation of untrusted input in Omnibox in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name. **CVE ID : CVE-2020-6401**	N/A	A-OPE-BACK-180220/236
Improper Input Validation	11-02-2020	6.8	Insufficient policy enforcement in downloads in Google Chrome on OS X prior to 80.0.3987.87 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted Chrome Extension. **CVE ID : CVE-2020-6402**	N/A	A-OPE-BACK-180220/237
Improper Input	11-02-2020	4.3	Incorrect implementation in Omnibox in Google Chrome on iOS prior to	N/A	A-OPE-BACK-180220/238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			80.0.3987.87 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. **CVE ID : CVE-2020-6403**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	4.6	Inappropriate implementation in Blink in Google Chrome prior to 80.0.3987.87 allowed a local attacker to potentially exploit heap corruption via crafted clipboard content. **CVE ID : CVE-2020-6404**	N/A	A-OPE-BACK-180220/239
Information Exposure	11-02-2020	2.1	Insufficient policy enforcement in CORS in Google Chrome prior to 80.0.3987.87 allowed a local attacker to obtain potentially sensitive information via a crafted HTML page. **CVE ID : CVE-2020-6408**	N/A	A-OPE-BACK-180220/240
Improper Input Validation	11-02-2020	5.8	Insufficient validation of untrusted input in Omnibox in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name. **CVE ID : CVE-2020-6412**	N/A	A-OPE-BACK-180220/241
N/A	11-02-2020	6.8	Inappropriate implementation in Blink in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass	N/A	A-OPE-BACK-180220/242

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HTML validators via a crafted HTML page. **CVE ID : CVE-2020-6413**		
N/A	11-02-2020	6.8	Insufficient policy enforcement in Safe Browsing in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. **CVE ID : CVE-2020-6414**	N/A	A-OPE-BACK-180220/243
wicked					
Missing Release of Resource after Effective Lifetime	05-02-2020	5	An ni_dhcp4_parse_response memory leak in openSUSE wicked 0.6.55 and earlier allows network attackers to cause a denial of service by sending DHCP4 packets without a message type option. **CVE ID : CVE-2020-7216**	http://lists.opensuse.org/opensuse-security-announce/2020-02/msg00005.html	A-OPE-WICK-180220/244
Missing Release of Resource after Effective Lifetime	11-02-2020	5	An ni_dhcp4_fsm_process_dhcp4_packet memory leak in openSUSE wicked 0.6.55 and earlier allows network attackers to cause a denial of service by sending DHCP4 packets with a different client-id. **CVE ID : CVE-2020-7217**	N/A	A-OPE-WICK-180220/245
opservices					
opmon					
Missing Authenticati on for	06-02-2020	5	An issue was discovered in OpServices OpMon 9.3.2. Without authentication, it	N/A	A-OPS-OPMO-180220/246

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Critical Function			is possible to read server files (e.g., /etc/passwd) due to the use of the nmap -iL (aka input file) option. **CVE ID : CVE-2020-7953**		
Improper Privilege Management	06-02-2020	7.2	An issue was discovered in OpServices OpMon 9.3.2. Starting from the apache user account, it is possible to perform privilege escalation through the lack of correct configuration in the server's sudoers file, which by default allows the execution of programs (e.g. nmap) without the need for a password with sudo. **CVE ID : CVE-2020-7954**	N/A	A-OPS-OPMO-180220/247
Missing Authenticati on for Critical Function	06-02-2020	10	An issue was discovered in OpServices OpMon 9.3.2 that allows Remote Code Execution . **CVE ID : CVE-2020-8636**	N/A	A-OPS-OPMO-180220/248
Otrs					
otrs					
Insufficient Session Expiration	07-02-2020	5.5	The external frontend system uses numerous background calls to the backend. Each background request is treated as user activity so the SessionMaxIdleTime will not be reached. This issue affects: OTRS 7.0.x version 7.0.14 and prior versions. **CVE ID : CVE-2020-1768**	https://otrs.com/release-notes/otrs-security-advisory-2020-04/	A-OTR-OTRS-180220/249
Percona					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
monitoring_and_management					
Uncontrolled Resource Consumption	06-02-2020	7.8	pmm-server in Percona Monitoring and Management (PMM) 2.2.x before 2.2.1 allows unauthenticated denial of service. **CVE ID : CVE-2020-7920**	N/A	A-PER-MONI-180220/250
PHP					
php					
Out-of-bounds Read	10-02-2020	6.4	When using fgetss() function to read data with stripping tags, in PHP versions 7.2.x below 7.2.27, 7.3.x below 7.3.14 and 7.4.x below 7.4.2 it is possible to supply data that will cause this function to read past the allocated buffer. This may lead to information disclosure or crash. **CVE ID : CVE-2020-7059**	N/A	A-PHP-PHP-180220/251
Out-of-bounds Read	10-02-2020	6.4	When using certain mbstring functions to convert multibyte encodings, in PHP versions 7.2.x below 7.2.27, 7.3.x below 7.3.14 and 7.4.x below 7.4.2 it is possible to supply data that will cause function mbfl_filt_conv_big5_wchar to read past the allocated buffer. This may lead to information disclosure or crash. **CVE ID : CVE-2020-7060**	N/A	A-PHP-PHP-180220/252

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
phpabook_project					
phpabook					
Improper Authentication	03-02-2020	7.5	An issue was discovered in phpABook 0.9 Intermediate. On the login page, if one sets a userInfo cookie with the value of admin+1+en (user+perms+lang), one can login as any user without a password. **CVE ID : CVE-2020-8510**	N/A	A-PHP-PHPA-180220/253
Phplist					
phplist					
Access of Resource Using Incompatible Type ('Type Confusion')	03-02-2020	7.5	phpList 3.5.0 allows type juggling for admin login bypass because == is used instead of === for password hashes, which mishandles hashes that begin with 0e followed by exclusively numerical characters. **CVE ID : CVE-2020-8547**	N/A	A-PHP-PHPL-180220/254
Piwigo					
piwigo					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-02-2020	3.5	Piwigo 2.10.1 is affected by stored XSS via the Group Name Field to the group_list page. **CVE ID : CVE-2020-8089**	https://github.com/Piwigo/Piwigo/issues/1150	A-PIW-PIWI-180220/255
Playsms					
playsms					
Improper	05-02-2020	7.5	PlaySMS before 1.4.3 does	N/A	A-PLA-PLAY-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			not sanitize inputs from a malicious string. **CVE ID : CVE-2020-8644**		180220/256
point-to-point_protocol_project					
point-to-point_protocol					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-02-2020	7.5	eap.c in pppd in ppp 2.4.2 through 2.4.8 has an rhostname buffer overflow in the eap_request and eap_response functions. **CVE ID : CVE-2020-8597**	N/A	A-POI-POIN-180220/257
Prototypejs					
prototype					
Improper Privilege Management	03-02-2020	4	Prototype 1.6.0.1 allows remote authenticated users to forge ticket creation (on behalf of other user accounts) via a modified email ID field. **CVE ID : CVE-2020-7993**	N/A	A-PRO-PROT-180220/258
Redhat					
keycloak					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-02-2020	3.5	It was found in all keycloak versions before 9.0.0 that links to external applications (Application Links) in the admin console are not validated properly and could allow Stored XSS attacks. An authed malicious user could create URLs to trick users in other realms, and possibly conduct further attacks. **CVE ID : CVE-2020-1697**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1697	A-RED-KEYC-180220/259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
single_sign-on					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-02-2020	3.5	It was found in all keycloak versions before 9.0.0 that links to external applications (Application Links) in the admin console are not validated properly and could allow Stored XSS attacks. An authed malicious user could create URLs to trick users in other realms, and possibly conduct further attacks. **CVE ID : CVE-2020-1697**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1697	A-RED-SING-180220/260
openshift_container_platform					
Improper Privilege Management	07-02-2020	4.4	It has been found in openshift-enterprise version 3.11 and all openshift-enterprise versions from 4.1 to, including 4.3, that multiple containers modify the permissions of /etc/passwd to make them modifiable by users other than root. An attacker with access to the running container can exploit this to modify /etc/passwd to add a user and escalate their privileges. This CVE is specific to the openshift/mysql-apb. **CVE ID : CVE-2020-1708**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1708	A-RED-OPEN-180220/261
openshift_container_storage					
Uncontrolled Resource Consumption	07-02-2020	6.8	A flaw was found in the way the Ceph RGW Beast front-end handles	https://bugzilla.redhat.com/show_bug	A-RED-OPEN-180220/262

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unexpected disconnects. An authenticated attacker can abuse this flaw by making multiple disconnect attempts resulting in a permanent leak of a socket connection by radosgw. This flaw could lead to a denial of service condition by pile up of CLOSE_WAIT sockets, eventually leading to the exhaustion of available resources, preventing legitimate users from connecting to the system. **CVE ID : CVE-2020-1700**	.cgi?id=CVE-2020-1700	
openshift_service_mesh					
Improper Authenticati on	12-02-2020	7.5	Istio 1.3 through 1.4.3 allows authentication bypass. The Authentication Policy exact-path matching logic can allow unauthorized access to HTTP paths even if they are configured to be only accessed after presenting a valid JWT token. For example, an attacker can add a ? or # character to a URI that would otherwise satisfy an exact-path match. **CVE ID : CVE-2020-8595**	https://acces s.redhat.com /security/cv e/cve-2020-8595, https://istio. io/news/sec urity/istio-security-2020-001/	A-RED-OPEN-180220/263
Revive-adserver					
revive_adserver					
Improper Neutralizatio	04-02-2020	4.3	A reflected XSS vulnerability has been	N/A	A-REV-REVI-180220/264

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			discovered in the publicly accessible afr.php delivery script of Revive Adserver <= 5.0.3 by Jacopo Tediosi. There are currently no known exploits: the session identifier cannot be accessed as it is stored in an http-only cookie as of v3.2.2. On older versions, however, under specific circumstances, it could be possible to steal the session identifier and gain access to the admin interface. The query string sent to the www/delivery/afr.php script was printed back without proper escaping in a JavaScript context, allowing an attacker to execute arbitrary JS code on the browser of the victim. **CVE ID : CVE-2020-8115**		
revmakx					
infinitewp_client					
Missing Authorization	06-02-2020	7.5	The InfiniteWP Client plugin before 1.9.4.5 for WordPress has a missing authorization check in iwp_mmb_set_request in init.php. Any attacker who knows the username of an administrator can log in. **CVE ID : CVE-2020-8772**	N/A	A-REV-INFI-180220/265
rogersmedia					
citytv_video					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	05-02-2020	5	The Citytv Video application 4.08.0 for Android and 3.35 for iOS sends Unencrypted Analytics. **CVE ID : CVE-2020-8507**	N/A	A-ROG-CITY-180220/266
secom					
dr.id_access_control					
Information Exposure	11-02-2020	5	Secom Co. Dr.ID, a Door Access Control and Personnel Attendance Management system, allows attackers to enumerate and exam user account in the system. **CVE ID : CVE-2020-3933**	N/A	A-SEC-DR.I-180220/267
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-02-2020	7.5	Secom Co. Dr.ID, a Door Access Control and Personnel Attendance Management system, contains a vulnerability of Pre-auth SQL Injection, allowing attackers to inject a specific SQL command. **CVE ID : CVE-2020-3934**	N/A	A-SEC-DR.I-180220/268
Cleartext Storage of Sensitive Information	11-02-2020	5	Secom Co. Dr.ID, a Door Access Control and Personnel Attendance Management system, stores users' information by cleartext in the cookie, which divulges password to attackers. **CVE ID : CVE-2020-3935**	N/A	A-SEC-DR.I-180220/269
dr.id_attendance_system					
Information Exposure	11-02-2020	5	Secom Co. Dr.ID, a Door Access Control and Personnel Attendance	N/A	A-SEC-DR.I-180220/270

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Management system, allows attackers to enumerate and exam user account in the system. **CVE ID : CVE-2020-3933**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-02-2020	7.5	Secom Co. Dr.ID, a Door Access Control and Personnel Attendance Management system, contains a vulnerability of Pre-auth SQL Injection, allowing attackers to inject a specific SQL command. **CVE ID : CVE-2020-3934**	N/A	A-SEC-DR.I-180220/271
Cleartext Storage of Sensitive Information	11-02-2020	5	Secom Co. Dr.ID, a Door Access Control and Personnel Attendance Management system, stores users' information by cleartext in the cookie, which divulges password to attackers. **CVE ID : CVE-2020-3935**	N/A	A-SEC-DR.I-180220/272
simplejobscript					
simplejobscript					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-02-2020	7.5	An issue was discovered in Simplejobscript.com SJS through 1.66. There is an unauthenticated SQL injection via the job applications search function. The vulnerable parameter is job_id. The function is getJobApplicationsByJobId(). The file is _lib/class.JobApplication.php.	N/A	A-SIM-SIMP-180220/273

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8645		
Sixapart					
movable_type					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-02-2020	4.3	Cross-site scripting vulnerability in Movable Type series (Movable Type 7 r.4603 and earlier (Movable Type 7), Movable Type 6.5.2 and earlier (Movable Type 6.5), Movable Type Advanced 7 r.4603 and earlier (Movable Type Advanced 7), Movable Type Advanced 6.5.2 and earlier (Movable Type Advanced 6.5), Movable Type Premium 1.26 and earlier (Movable Type Premium), and Movable Type Premium Advanced 1.26 and earlier (Movable Type Premium Advanced)) allows remote attackers to inject arbitrary web script or HTML in the block editor and the rich text editor via a specially crafted URL. **CVE ID : CVE-2020-5528**	N/A	A-SIX-MOVA-180220/274
sockjs_project					
sockjs					
Improper Neutralization of Input During Web Page Generation ('Cross-site	10-02-2020	4.3	htmlfile in lib/transport/htmlfile.js in SockJS before 3.0 is vulnerable to Reflected XSS via the /htmlfile c (aka callback) parameter.	N/A	A-SOC-SOCK-180220/275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			**CVE ID : CVE-2020-8823**		
sos-berlin					
jobscheduler					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-02-2020	3.5	A cross-site scripting (XSS) vulnerability in the JOC Cockpit component of SOS JobScheduler 1.11 and 1.13.2 allows attackers to inject arbitrary web script or HTML via JSON properties available from the REST API. **CVE ID : CVE-2020-6854**	N/A	A-SOS-JOBS-180220/276
Loop with Unreachable Exit Condition ('Infinite Loop')	06-02-2020	6.8	A large or infinite loop vulnerability in the JOC Cockpit component of SOS JobScheduler 1.11 and 1.13.2 allows attackers to parameterize housekeeping jobs in a way that exhausts system resources and results in a denial of service. **CVE ID : CVE-2020-6855**	N/A	A-SOS-JOBS-180220/277
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	06-02-2020	4	An XML External Entity (XEE) vulnerability exists in the JOC Cockpit component of SOS JobScheduler 1.12 and 1.13.2 allows attackers to read files from the server via an entity declaration in any of the XML documents that are used to specify the run-time settings of jobs and orders. **CVE ID : CVE-2020-6856**	N/A	A-SOS-JOBS-180220/278
Squid-cache					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
squid					
Improper Input Validation	04-02-2020	5	An issue was discovered in Squid before 4.10. Due to incorrect input validation, it can interpret crafted HTTP requests in unexpected ways to access server resources prohibited by earlier security filters. **CVE ID : CVE-2020-8449**	N/A	A-SQU-SQUI-180220/279
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-02-2020	7.5	An issue was discovered in Squid before 4.10. Due to incorrect buffer management, a remote client can cause a buffer overflow in a Squid instance acting as a reverse proxy. **CVE ID : CVE-2020-8450**	N/A	A-SQU-SQUI-180220/280
Improper Input Validation	04-02-2020	5	An issue was discovered in Squid before 4.10. Due to incorrect input validation, the NTLM authentication credentials parser in ext_lm_group_acl may write to memory outside the credentials buffer. On systems with memory access protections, this can result in the helper process being terminated unexpectedly. This leads to the Squid process also terminating and a denial of service for all clients using the proxy. **CVE ID : CVE-2020-8517**	N/A	A-SQU-SQUI-180220/281
strapi					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
strapi					
Uncontrolled Resource Consumption	04-02-2020	4	A denial of service exists in strapi v3.0.0-beta.18.3 and earlier that can be abused in the admin console using admin rights can lead to arbitrary restart of the application. **CVE ID : CVE-2020-8123**	N/A	A-STR-STRA-180220/282
Symantec					
endpoint_protection					
Improper Privilege Management	11-02-2020	4.6	Symantec Endpoint Protection (SEP) and Symantec Endpoint Protection Small Business Edition (SEP SBE), prior to 14.2 RU2 MP1 and prior to 14.2.5569.2100 respectively, may be susceptible to a privilege escalation vulnerability, which is a type of issue whereby an attacker may attempt to compromise the software application to gain elevated access to resources that are normally protected from an application or user. **CVE ID : CVE-2020-5820**	N/A	A-SYM-ENDP-180220/283
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	11-02-2020	4.6	Symantec Endpoint Protection (SEP) and Symantec Endpoint Protection Small Business Edition (SEP SBE), prior to 14.2 RU2 MP1 and prior to 14.2.5569.2100 respectively, may be susceptible to a DLL	N/A	A-SYM-ENDP-180220/284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			injection vulnerability, which is a type of issue whereby an individual attempts to execute their own code in place of legitimate code as a means to perform an exploit. **CVE ID : CVE-2020-5821**		
Improper Privilege Management	11-02-2020	4.6	Symantec Endpoint Protection (SEP) and Symantec Endpoint Protection Small Business Edition (SEP SBE), prior to 14.2 RU2 MP1 and prior to 14.2.5569.2100 respectively, may be susceptible to a privilege escalation vulnerability, which is a type of issue whereby an attacker may attempt to compromise the software application to gain elevated access to resources that are normally protected from an application or user. **CVE ID : CVE-2020-5822**	N/A	A-SYM-ENDP-180220/285
Improper Privilege Management	11-02-2020	4.6	Symantec Endpoint Protection (SEP) and Symantec Endpoint Protection Small Business Edition (SEP SBE), prior to 14.2 RU2 MP1 and prior to 14.2.5569.2100 respectively, may be susceptible to a privilege escalation vulnerability, which is a type of issue whereby an attacker may attempt to compromise	N/A	A-SYM-ENDP-180220/286

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the software application to gain elevated access to resources that are normally protected from an application or user. **CVE ID : CVE-2020-5823**		
N/A	11-02-2020	2.1	Symantec Endpoint Protection (SEP) and Symantec Endpoint Protection Small Business Edition (SEP SBE), prior to 14.2 RU2 MP1 and prior to 14.2.5569.2100 respectively, may be susceptible to a denial of service vulnerability, which is a type of issue whereby a threat actor attempts to tie up the resources of a resident application, thereby making certain functions unavailable. **CVE ID : CVE-2020-5824**	N/A	A-SYM-ENDP-180220/287
Improper Privilege Management	11-02-2020	3.6	Symantec Endpoint Protection (SEP) and Symantec Endpoint Protection Small Business Edition (SEP SBE), prior to 14.2 RU2 MP1 and prior to 14.2.5569.2100 respectively, may be susceptible to an arbitrary file write vulnerability, which is a type of issue whereby an attacker is able to overwrite existing files on the resident system without proper privileges.	N/A	A-SYM-ENDP-180220/288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5825		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	Symantec Endpoint Protection (SEP) and Symantec Endpoint Protection Small Business Edition (SEP SBE), prior to 14.2 RU2 MP1 and prior to 14.2.5569.2100 respectively, may be susceptible to an out of bounds vulnerability, which is a type of issue that results in an existing application reading memory outside of the bounds of the memory that had been allocated to the program. **CVE ID : CVE-2020-5826**	N/A	A-SYM-ENDP-180220/289
endpoint_protection_manager					
Out-of-bounds Read	11-02-2020	2.1	Symantec Endpoint Protection Manager (SEPM), prior to 14.2 RU2 MP1, may be susceptible to an out of bounds vulnerability, which is a type of issue that results in an existing application reading memory outside of the bounds of the memory that had been allocated to the program. **CVE ID : CVE-2020-5827**	N/A	A-SYM-ENDP-180220/290
Out-of-bounds Read	11-02-2020	2.1	Symantec Endpoint Protection Manager (SEPM), prior to 14.2 RU2 MP1, may be susceptible to an out of bounds vulnerability, which is a	N/A	A-SYM-ENDP-180220/291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			type of issue that results in an existing application reading memory outside of the bounds of the memory that had been allocated to the program. **CVE ID : CVE-2020-5828**		
Out-of-bounds Read	11-02-2020	2.1	Symantec Endpoint Protection Manager (SEPM), prior to 14.2 RU2 MP1, may be susceptible to an out of bounds vulnerability, which is a type of issue that results in an existing application reading memory outside of the bounds of the memory that had been allocated to the program. **CVE ID : CVE-2020-5829**	N/A	A-SYM-ENDP-180220/292
Out-of-bounds Read	11-02-2020	2.1	Symantec Endpoint Protection Manager (SEPM), prior to 14.2 RU2 MP1, may be susceptible to an out of bounds vulnerability, which is a type of issue that results in an existing application reading memory outside of the bounds of the memory that had been allocated to the program. **CVE ID : CVE-2020-5830**	N/A	A-SYM-ENDP-180220/293
Out-of-bounds Read	11-02-2020	2.1	Symantec Endpoint Protection Manager (SEPM), prior to 14.2 RU2 MP1, may be susceptible to an out of bounds vulnerability, which is a	N/A	A-SYM-ENDP-180220/294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			type of issue that results in an existing application reading memory outside of the bounds of the memory that had been allocated to the program. **CVE ID : CVE-2020-5831**		
synaptivemedical					
clearcanvas					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-02-2020	4.3	Synaptive Medical ClearCanvas ImageServer 3.0 Alpha allows XSS (and HTML injection) via the Default.aspx UserName parameter. NOTE: the issues/227 reference does not imply that the affected product can be downloaded from GitHub. It was simply a convenient location for a public bug report. **CVE ID : CVE-2020-8788**	N/A	A-SYN-CLEA-180220/295
sysjust					
syuan-gu-da-shin					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-02-2020	5	SQL Injection in SysJust Syuan-Gu-Da-Shih, versions before 20191223, allowing attackers to perform unwanted SQL queries and access arbitrary file in the database. **CVE ID : CVE-2020-3937**	N/A	A-SYS-SYUA-180220/296
Server-Side Request Forgery (SSRF)	04-02-2020	5	SysJust Syuan-Gu-Da-Shih, versions before 20191223, contain vulnerability of Request Forgery, allowing	N/A	A-SYS-SYUA-180220/297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers to launch inquiries into network architecture or system files of the server via forged inquests. **CVE ID : CVE-2020-3938**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-02-2020	4.3	SysJust Syuan-Gu-Da-Shih, versions before 20191223, contain vulnerability of Cross-Site Scripting(XSS), personal information may be leaked to attackers via the vulnerability. **CVE ID : CVE-2020-3939**	N/A	A-SYS-SYUA-180220/298
Testlink					
testlink					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-02-2020	6.5	An issue was discovered in TestLink 1.9.19. The relation_type parameter of the lib/requirements/reqSearch.php endpoint is vulnerable to authenticated SQL Injection. **CVE ID : CVE-2020-8841**	N/A	A-TES-TEST-180220/299
themeum					
tutor_lms					
Cross-Site Request Forgery (CSRF)	04-02-2020	2.6	A CSRF vulnerability in the Tutor LMS plugin before 1.5.3 for WordPress can result in an attacker approving themselves as an instructor and performing other malicious actions (such as blocking legitimate instructors).	N/A	A-THE-TUTO-180220/300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8615		
Torproject					
tor					
Information Exposure	02-02-2020	5	** DISPUTED ** The daemon in Tor through 0.4.1.8 and 0.4.2.x through 0.4.2.6 does not verify that a rendezvous node is known before attempting to connect to it, which might make it easier for remote attackers to discover circuit information. NOTE: The network team of Tor claims this is an intended behavior and not a vulnerability. **CVE ID : CVE-2020-8516**	N/A	A-TOR-TOR-180220/301
url-parse_project					
url-parse					
Improper Input Validation	04-02-2020	5	Insufficient validation and sanitization of user input exists in url-parse npm package version 1.4.4 and earlier may allow attacker to bypass security checks. **CVE ID : CVE-2020-8124**	N/A	A-URL-URL--180220/302
Vanillaforums					
vanilla					
Improper Neutralization of Input During Web Page Generation ('Cross-site	10-02-2020	3.5	index.php?p=/dashboard/settings/branding in Vanilla 2.6.3 allows stored XSS. **CVE ID : CVE-2020-8825**	N/A	A-VAN-VANI-180220/303

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')					
wptimecapsule					
wp_time_capsule					
Improper Authentication	06-02-2020	7.5	The Time Capsule plugin before 1.21.16 for WordPress has an authentication bypass. Any request containing IWP_JSON_PREFIX causes the client to be logged in as the first account on the list of administrator accounts. **CVE ID : CVE-2020-8771**	N/A	A-WPT-WP_T-180220/304
Operating System					
Apple					
mac_os					
Improper Input Validation	11-02-2020	6.8	Insufficient policy enforcement in downloads in Google Chrome on OS X prior to 80.0.3987.87 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted Chrome Extension. **CVE ID : CVE-2020-6402**	N/A	O-APP-MAC_-180220/305
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-02-2020	4.3	An issue was discovered in Rumpus 8.2.10 on macOS. By crafting a directory name, it is possible to activate JavaScript in the context of the web application after invoking the rename folder functionality. **CVE ID : CVE-2020-8514**	N/A	O-APP-MAC_-180220/306

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
iphone_os					
Improper Input Validation	11-02-2020	4.3	Incorrect implementation in Omnibox in Google Chrome on iOS prior to 80.0.3987.87 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. **CVE ID : CVE-2020-6403**	N/A	O-APP-IPHO-180220/307
automationdirect					
c-more_ea9-rhi_firmware					
Insufficiently Protected Credentials	05-02-2020	10	It is possible to unmask credentials and other sensitive information on “unprotected” project files, which may allow an attacker to remotely access the C-More Touch Panels EA9 series: firmware versions prior to 6.53 and manipulate system configurations. **CVE ID : CVE-2020-6969**	N/A	O-AUT-C-MO-180220/308
c-more_ea9-t6cl-r_firmware					
Insufficiently Protected Credentials	05-02-2020	10	It is possible to unmask credentials and other sensitive information on “unprotected” project files, which may allow an attacker to remotely access the C-More Touch Panels EA9 series: firmware versions prior to 6.53 and manipulate system configurations. **CVE ID : CVE-2020-6969**	N/A	O-AUT-C-MO-180220/309
c-more_ea9-t6cl_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	05-02-2020	10	It is possible to unmask credentials and other sensitive information on "unprotected" project files, which may allow an attacker to remotely access the C-More Touch Panels EA9 series: firmware versions prior to 6.53 and manipulate system configurations. **CVE ID : CVE-2020-6969**	N/A	O-AUT-C-MO-180220/310
c-more_ea9-t7cl-r_firmware					
Insufficiently Protected Credentials	05-02-2020	10	It is possible to unmask credentials and other sensitive information on "unprotected" project files, which may allow an attacker to remotely access the C-More Touch Panels EA9 series: firmware versions prior to 6.53 and manipulate system configurations. **CVE ID : CVE-2020-6969**	N/A	O-AUT-C-MO-180220/311
c-more_ea9-t7cl_firmware					
Insufficiently Protected Credentials	05-02-2020	10	It is possible to unmask credentials and other sensitive information on "unprotected" project files, which may allow an attacker to remotely access the C-More Touch Panels EA9 series: firmware versions prior to 6.53 and manipulate system configurations. **CVE ID : CVE-2020-6969**	N/A	O-AUT-C-MO-180220/312

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
c-more_ea9-t8cl_firmware					
Insufficiently Protected Credentials	05-02-2020	10	It is possible to unmask credentials and other sensitive information on "unprotected" project files, which may allow an attacker to remotely access the C-More Touch Panels EA9 series: firmware versions prior to 6.53 and manipulate system configurations. **CVE ID : CVE-2020-6969**	N/A	O-AUT-C-MO-180220/313
c-more_ea9-t10cl_firmware					
Insufficiently Protected Credentials	05-02-2020	10	It is possible to unmask credentials and other sensitive information on "unprotected" project files, which may allow an attacker to remotely access the C-More Touch Panels EA9 series: firmware versions prior to 6.53 and manipulate system configurations. **CVE ID : CVE-2020-6969**	N/A	O-AUT-C-MO-180220/314
c-more_ea9-t10wcl_firmware					
Insufficiently Protected Credentials	05-02-2020	10	It is possible to unmask credentials and other sensitive information on "unprotected" project files, which may allow an attacker to remotely access the C-More Touch Panels EA9 series: firmware versions prior to 6.53 and manipulate system configurations.	N/A	O-AUT-C-MO-180220/315

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-6969		
c-more_ea9-t12cl_firmware					
Insufficiently Protected Credentials	05-02-2020	10	It is possible to unmask credentials and other sensitive information on "unprotected" project files, which may allow an attacker to remotely access the C-More Touch Panels EA9 series: firmware versions prior to 6.53 and manipulate system configurations. **CVE ID : CVE-2020-6969**	N/A	O-AUT-C-MO-180220/316
c-more_ea9-t15cl-r_firmware					
Insufficiently Protected Credentials	05-02-2020	10	It is possible to unmask credentials and other sensitive information on "unprotected" project files, which may allow an attacker to remotely access the C-More Touch Panels EA9 series: firmware versions prior to 6.53 and manipulate system configurations. **CVE ID : CVE-2020-6969**	N/A	O-AUT-C-MO-180220/317
c-more_ea9-t15cl_firmware					
Insufficiently Protected Credentials	05-02-2020	10	It is possible to unmask credentials and other sensitive information on "unprotected" project files, which may allow an attacker to remotely access the C-More Touch Panels EA9 series: firmware versions prior to 6.53 and manipulate	N/A	O-AUT-C-MO-180220/318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system configurations. **CVE ID : CVE-2020-6969**		
bosch					
divar_ip_2000_firmware					
Missing Authenticati on for Critical Function	07-02-2020	6.4	Missing Authentication for Critical Function in the Bosch Video Streaming Gateway (VSG) allows an unauthenticated remote attacker to retrieve and set arbitrary configuration data of the Video Streaming Gateway. A successful attack can impact the confidentiality and availability of live and recorded video data of all cameras configured to be controlled by the VSG as well as the recording storage associated with the VSG. This affects Bosch Video Streaming Gateway versions 6.45 <= 6.45.08, 6.44 <= 6.44.022, 6.43 <= 6.43.0023 and 6.42.10 and older. This affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR IP all-in-one 5000 if a vulnerable VSG version is installed with BVMS. This affects Bosch DIVAR IP 2000 <= 3.62.0019 and DIVAR IP 5000 <= 3.80.0039 if the corresponding port 8023 has been opened in the device's firewall. **CVE ID : CVE-2020-6769**	https://psirt.bosch.com/security-advisories/BOSCH-SA-260625-BT.html	O-BOS-DIVA-180220/319

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
divar_ip_5000_firmware					
Missing Authentication for Critical Function	07-02-2020	6.4	Missing Authentication for Critical Function in the Bosch Video Streaming Gateway (VSG) allows an unauthenticated remote attacker to retrieve and set arbitrary configuration data of the Video Streaming Gateway. A successful attack can impact the confidentiality and availability of live and recorded video data of all cameras configured to be controlled by the VSG as well as the recording storage associated with the VSG. This affects Bosch Video Streaming Gateway versions 6.45 <= 6.45.08, 6.44 <= 6.44.022, 6.43 <= 6.43.0023 and 6.42.10 and older. This affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR IP all-in-one 5000 if a vulnerable VSG version is installed with BVMS. This affects Bosch DIVAR IP 2000 <= 3.62.0019 and DIVAR IP 5000 <= 3.80.0039 if the corresponding port 8023 has been opened in the device's firewall. **CVE ID : CVE-2020-6769**	https://psirt.bosch.com/security-advisories/BOSCH-SA-260625-BT.html	O-BOS-DIVA-180220/320
divar_ip_3000_firmware					
Deserialization of Untrusted	07-02-2020	10	Deserialization of Untrusted Data in the BVMS Mobile Video	https://psirt.bosch.com/security-	O-BOS-DIVA-180220/321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Data			Service (BVMS MVS) allows an unauthenticated remote attacker to execute arbitrary code on the system. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000 and DIVAR IP 7000 if a vulnerable BVMS version is installed. **CVE ID : CVE-2020-6770**	advisories/BOSCH-SA-885551-BT.html	
divar_ip_7000_firmware					
Deserialization of Untrusted Data	07-02-2020	10	Deserialization of Untrusted Data in the BVMS Mobile Video Service (BVMS MVS) allows an unauthenticated remote attacker to execute arbitrary code on the system. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000 and DIVAR IP 7000 if a vulnerable BVMS version is installed. **CVE ID : CVE-2020-6770**	https://psirt.bosch.com/security-advisories/BOSCH-SA-885551-BT.html	O-BOS-DIVA-180220/322
Cisco					
ip_conference_phone_7832_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated,	N/A	O-CIS-IP_C-180220/323

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
ip_conference_phone_8832_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an	N/A	O-CIS-IP_C-180220/324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
ip_phone_7811_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery	N/A	O-CIS-IP_P-180220/325

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
ip_phone_7821_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery	N/A	O-CIS-IP_P-180220/326

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
ip_phone_7841_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to	N/A	O-CIS-IP_P-180220/327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
ip_phone_7861_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone,	N/A	O-CIS-IP_P-180220/328

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
ip_phone_8811_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To	N/A	O-CIS-IP_P-180220/329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
ip_phone_8841_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer	N/A	O-CIS-IP_P-180220/330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2 adjacent). **CVE ID : CVE-2020-3111**		
ip_phone_8845_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**	N/A	O-CIS-IP_P-180220/331
ip_phone_8851_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**	N/A	O-CIS-IP_P-180220/332
ip_phone_8861_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow	N/A	O-CIS-IP_P-180220/333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
ip_phone_8865_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or	N/A	O-CIS-IP_P-180220/334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
wireless_ip_phone_8821-ex_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when	N/A	O-CIS-WIRE-180220/335

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
wireless_ip_phone_8821_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a	N/A	O-CIS-WIRE-180220/336

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
fxos					
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an	N/A	O-CIS-FXOS-180220/337

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nx-os					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to	N/A	O-CIS-NX-O-180220/338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker	N/A	O-CIS-NX-O-180220/339

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
video_surveillance_8400_ip_camera_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco Video Surveillance 8000 Series IP Cameras could allow an unauthenticated, adjacent attacker to execute code remotely or cause a reload of an affected IP Camera. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to the targeted IP Camera. A successful exploit could allow the attacker to expose the affected IP Camera for remote code execution or cause it to reload unexpectedly, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). This	N/A	O-CIS-VIDE-180220/340

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is fixed in Video Surveillance 8000 Series IP Camera Firmware Release 1.0.7 and later. **CVE ID : CVE-2020-3110**		
video_surveillance_8030_ip_camera_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco Video Surveillance 8000 Series IP Cameras could allow an unauthenticated, adjacent attacker to execute code remotely or cause a reload of an affected IP Camera. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to the targeted IP Camera. A successful exploit could allow the attacker to expose the affected IP Camera for remote code execution or cause it to reload unexpectedly, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer	N/A	O-CIS-VIDE-180220/341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2 adjacent). This vulnerability is fixed in Video Surveillance 8000 Series IP Camera Firmware Release 1.0.7 and later. **CVE ID : CVE-2020-3110**		
video_surveillance_8020_ip_camera_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco Video Surveillance 8000 Series IP Cameras could allow an unauthenticated, adjacent attacker to execute code remotely or cause a reload of an affected IP Camera. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to the targeted IP Camera. A successful exploit could allow the attacker to expose the affected IP Camera for remote code execution or cause it to reload unexpectedly, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as	N/A	O-CIS-VIDE-180220/342

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the affected device (Layer 2 adjacent). This vulnerability is fixed in Video Surveillance 8000 Series IP Camera Firmware Release 1.0.7 and later. **CVE ID : CVE-2020-3110**		
video_surveillance_8000p_ip_camera_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco Video Surveillance 8000 Series IP Cameras could allow an unauthenticated, adjacent attacker to execute code remotely or cause a reload of an affected IP Camera. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to the targeted IP Camera. A successful exploit could allow the attacker to expose the affected IP Camera for remote code execution or cause it to reload unexpectedly, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the	N/A	O-CIS-VIDE-180220/343

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			same broadcast domain as the affected device (Layer 2 adjacent). This vulnerability is fixed in Video Surveillance 8000 Series IP Camera Firmware Release 1.0.7 and later. **CVE ID : CVE-2020-3110**		
video_surveillance_8930_speed_dome_ip_camera_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco Video Surveillance 8000 Series IP Cameras could allow an unauthenticated, adjacent attacker to execute code remotely or cause a reload of an affected IP Camera. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to the targeted IP Camera. A successful exploit could allow the attacker to expose the affected IP Camera for remote code execution or cause it to reload unexpectedly, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability,	N/A	O-CIS-VIDE-180220/344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). This vulnerability is fixed in Video Surveillance 8000 Series IP Camera Firmware Release 1.0.7 and later. **CVE ID : CVE-2020-3110**		
video_surveillance_8630_ip_camera_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco Video Surveillance 8000 Series IP Cameras could allow an unauthenticated, adjacent attacker to execute code remotely or cause a reload of an affected IP Camera. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to the targeted IP Camera. A successful exploit could allow the attacker to expose the affected IP Camera for remote code execution or cause it to reload unexpectedly, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To	N/A	O-CIS-VIDE-180220/345

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). This vulnerability is fixed in Video Surveillance 8000 Series IP Camera Firmware Release 1.0.7 and later. **CVE ID : CVE-2020-3110**		
video_surveillance_8070_ip_camera_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco Video Surveillance 8000 Series IP Cameras could allow an unauthenticated, adjacent attacker to execute code remotely or cause a reload of an affected IP Camera. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to the targeted IP Camera. A successful exploit could allow the attacker to expose the affected IP Camera for remote code execution or cause it to reload unexpectedly, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is	N/A	O-CIS-VIDE-180220/346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). This vulnerability is fixed in Video Surveillance 8000 Series IP Camera Firmware Release 1.0.7 and later. **CVE ID : CVE-2020-3110**		
video_surveillance_8620_ip_camera_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco Video Surveillance 8000 Series IP Cameras could allow an unauthenticated, adjacent attacker to execute code remotely or cause a reload of an affected IP Camera. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to the targeted IP Camera. A successful exploit could allow the attacker to expose the affected IP Camera for remote code execution or cause it to reload unexpectedly, resulting in a denial of service (DoS) condition.	N/A	O-CIS-VIDE-180220/347

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). This vulnerability is fixed in Video Surveillance 8000 Series IP Camera Firmware Release 1.0.7 and later. **CVE ID : CVE-2020-3110**		
ip_conference_phone_7832_with_multiplatform_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of	N/A	O-CIS-IP_C-180220/348

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
ip_conference_phone_8832_with_multiplatform_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability,	N/A	O-CIS-IP_C-180220/349

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
ip_phone_6821_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	N/A	O-CIS-IP_P-180220/350

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3111		
ip_phone_6841_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**	N/A	O-CIS-IP_P-180220/351
ios_xr					
Use of Externally-	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol	N/A	O-CIS-IOS_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Controlled Format String			implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**		180220/352
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload	N/A	O-CIS-IOS_-180220/353

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
ip_phone_6851_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery	N/A	O-CIS-IP_P-180220/354

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
ip_phone_6861_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery	N/A	O-CIS-IP_P-180220/355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
ip_phone_6871_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to	N/A	O-CIS-IP_P-180220/356

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
ip_phone_7811_with_multiplatform_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone,	N/A	O-CIS-IP_P-180220/357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
ip_phone_7821_with_multiplatform_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To	N/A	O-CIS-IP_P-180220/358

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
ip_phone_7841_with_multiplatform_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer	N/A	O-CIS-IP_P-180220/359

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2 adjacent). **CVE ID : CVE-2020-3111**		
ip_phone_7861_with_multiplatform_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**	N/A	O-CIS-IP_P-180220/360
ip_phone_8811_with_multiplatform_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**	N/A	O-CIS-IP_P-180220/361
ip_phone_8841_with_multiplatform_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow	N/A	O-CIS-IP_P-180220/362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
ip_phone_8851_with_multiplatform_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or	N/A	O-CIS-IP_P-180220/363

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
ip_phone_8861_with_multiplatform_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when	N/A	O-CIS-IP_P-180220/364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
ip_phone_8845_with_multiplatform_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a	N/A	O-CIS-IP_P-180220/365

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
ip_phone_8865_with_multiplatform_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could	N/A	O-CIS-IP_P-180220/366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
unified_ip_conference_phone_8831_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an	N/A	O-CIS-UNIF-180220/367

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
unified_ip_conference_phone_8831_for_third-party_call_control_firmware					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is	N/A	O-CIS-UNIF-180220/368

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
Digi					
transport_wr21_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-02-2020	3.5	Digi TransPort WR21 5.2.2.3, WR44 5.1.6.4, and WR44v2 5.1.6.9 devices allow stored XSS in the web application. **CVE ID : CVE-2020-8822**	N/A	O-DIG-TRAN-180220/369
transport_wr44_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-02-2020	3.5	Digi TransPort WR21 5.2.2.3, WR44 5.1.6.4, and WR44v2 5.1.6.9 devices allow stored XSS in the web application. **CVE ID : CVE-2020-8822**	N/A	O-DIG-TRAN-180220/370
Draytek					
vigor2960_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	01-02-2020	10	DrayTek Vigor2960 1.3.1_Beta, Vigor3900 1.4.4_Beta, and Vigor300B 1.3.3_Beta, 1.4.2.1_Beta, and 1.4.4_Beta devices allow remote code execution as root (without authentication) via shell metacharacters to the cgi-bin/mainfunction.cgi URI.	N/A	O-DRA-VIGO-180220/371

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This issue has been fixed in Vigor3900/2960/300B v1.5.1. **CVE ID : CVE-2020-8515**		
vigor300b_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	01-02-2020	10	DrayTek Vigor2960 1.3.1_Beta, Vigor3900 1.4.4_Beta, and Vigor300B 1.3.3_Beta, 1.4.2.1_Beta, and 1.4.4_Beta devices allow remote code execution as root (without authentication) via shell metacharacters to the cgi-bin/mainfunction.cgi URI. This issue has been fixed in Vigor3900/2960/300B v1.5.1. **CVE ID : CVE-2020-8515**	N/A	O-DRA-VIGO-180220/372
vigor3900_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	01-02-2020	10	DrayTek Vigor2960 1.3.1_Beta, Vigor3900 1.4.4_Beta, and Vigor300B 1.3.3_Beta, 1.4.2.1_Beta, and 1.4.4_Beta devices allow remote code execution as root (without authentication) via shell metacharacters to the cgi-bin/mainfunction.cgi URI. This issue has been fixed in Vigor3900/2960/300B v1.5.1. **CVE ID : CVE-2020-8515**	N/A	O-DRA-VIGO-180220/373
Linux					
linux_kernel					
Use After Free	06-02-2020	3.6	There is a use-after-free vulnerability in the Linux	N/A	O-LIN-LINU-180220/374

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			kernel through 5.5.2 in the vc_do_resize function in drivers/tty/vt/vt.c. **CVE ID : CVE-2020-8647**		
Use After Free	06-02-2020	3.6	There is a use-after-free vulnerability in the Linux kernel through 5.5.2 in the n_tty_receive_buf_common function in drivers/tty/n_tty.c. **CVE ID : CVE-2020-8648**	N/A	O-LIN-LINU-180220/375
Use After Free	06-02-2020	3.6	There is a use-after-free vulnerability in the Linux kernel through 5.5.2 in the vgacon_invert_region function in drivers/video/console/vgacon.c. **CVE ID : CVE-2020-8649**	N/A	O-LIN-LINU-180220/376
Microsoft					
windows					
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3720**	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	O-MIC-WIND-180220/377
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3721**	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	O-MIC-WIND-180220/378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3722**	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	O-MIC-WIND-180220/379
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3723**	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	O-MIC-WIND-180220/380
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3724**	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	O-MIC-WIND-180220/381
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3725**	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	O-MIC-WIND-180220/382
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	O-MIC-WIND-180220/383

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2020-3726**		
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3727**	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	O-MIC-WIND-180220/384
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3728**	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	O-MIC-WIND-180220/385
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3729**	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	O-MIC-WIND-180220/386
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3730**	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	O-MIC-WIND-180220/387
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have a heap overflow vulnerability.	https://helpx.adobe.com/security/products/fram	O-MIC-WIND-180220/388

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3731**	emaker/apsb20-04.html	
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3732**	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	O-MIC-WIND-180220/389
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3733**	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	O-MIC-WIND-180220/390
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3734**	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	O-MIC-WIND-180220/391
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3735**	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	O-MIC-WIND-180220/392
Out-of-bounds Write	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have an out-of-	https://helpx.adobe.com/security/pr	O-MIC-WIND-180220/393

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3736**	oducts/framemaker/apsb20-04.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-02-2020	6.8	Adobe Framemaker versions 2019.0.4 and below have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3739**	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	O-MIC-WIND-180220/394
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-02-2020	10	Adobe Framemaker versions 2019.0.4 and below have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-3740**	https://helpx.adobe.com/security/products/framemaker/apsb20-04.html	O-MIC-WIND-180220/395
N/A	03-02-2020	9.3	A Remote Code Execution(RCE) vulnerability exists in some designated applications in ServiSign security plugin, as long as the interface is captured, attackers are able to launch RCE and executes arbitrary command on target system via malicious crafted scripts. **CVE ID : CVE-2020-3925**	https://tvn.twcert.org.tw/taiwanvn/TVN-201910005	O-MIC-WIND-180220/396
Files or Directories Accessible to External	03-02-2020	7.8	An arbitrary-file-access vulnerability exists in ServiSign security plugin, as long as the attackers learn the specific API	https://tvn.twcert.org.tw/taiwanvn/TVN-	O-MIC-WIND-180220/397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Parties			function, they may access arbitrary files on target system via crafted API parameter. **CVE ID : CVE-2020-3926**	201910006	
Files or Directories Accessible to External Parties	03-02-2020	8.5	An arbitrary-file-access vulnerability exists in ServiSign security plugin, as long as the attackers learn the specific API function, they may access arbitrary files on target system via crafted API parameter. **CVE ID : CVE-2020-3927**	https://tvn.twcert.org.tw/taiwanvn/TVN-201910007	O-MIC-WIND-180220/398
Incorrect Authorization	06-02-2020	4.6	When the Windows Logon Integration feature is configured for all versions of BIG-IP Edge Client for Windows, unauthorized users who have physical access to an authorized user's machine can get shell access under unprivileged user. **CVE ID : CVE-2020-5855**	https://support.f5.com/csp/article/K55102004	O-MIC-WIND-180220/399
windows_10					
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713, CVE-	N/A	O-MIC-WIND-180220/400

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-0767. **CVE ID : CVE-2020-0710**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0710, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767. **CVE ID : CVE-2020-0711**	N/A	O-MIC-WIND-180220/401
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0710, CVE-2020-0711, CVE-2020-0713, CVE-2020-0767. **CVE ID : CVE-2020-0712**	N/A	O-MIC-WIND-180220/402
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-	N/A	O-MIC-WIND-180220/403

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-0674, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0767. **CVE ID : CVE-2020-0713**		
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0717. **CVE ID : CVE-2020-0716**	N/A	O-MIC-WIND-180220/404
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0716. **CVE ID : CVE-2020-0717**	N/A	O-MIC-WIND-180220/405
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-	N/A	O-MIC-WIND-180220/406

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0719**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0720**	N/A	O-MIC-WIND-180220/407
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0721**	N/A	O-MIC-WIND-180220/408
Improper Privilege	11-02-2020	7.2	An elevation of privilege vulnerability exists in	N/A	O-MIC-WIND-180220/409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0722**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0723**	N/A	O-MIC-WIND-180220/410
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID	N/A	O-MIC-WIND-180220/411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0724**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0725**	N/A	O-MIC-WIND-180220/412
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-	N/A	O-MIC-WIND-180220/413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-0725, CVE-2020-0731. **CVE ID : CVE-2020-0726**		
N/A	11-02-2020	6.8	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-0729**	N/A	O-MIC-WIND-180220/414
Improper Link Resolution Before File Access ('Link Following')	11-02-2020	3.6	An elevation of privilege vulnerability exists when the Windows User Profile Service (ProfSvc) improperly handles symlinks, aka 'Windows User Profile Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0730**	N/A	O-MIC-WIND-180220/415
Improper Input Validation	11-02-2020	8.5	A remote code execution vulnerability exists in Remote Desktop Services â€“ formerly known as Terminal Services â€“ when an authenticated attacker abuses clipboard redirection, aka 'Remote Desktop ServicesÂ Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-0655**	N/A	O-MIC-WIND-180220/416

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory, aka 'Windows Common Log File System Driver Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0657**	N/A	O-MIC-WIND-180220/417
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists in the Windows Common Log File System (CLFS) driver when it fails to properly handle objects in memory, aka 'Windows Common Log File System Driver Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0658**	N/A	O-MIC-WIND-180220/418
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka 'Windows Data Sharing Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0747. **CVE ID : CVE-2020-0659**	N/A	O-MIC-WIND-180220/419
Improper Input Validation	11-02-2020	5	A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and	N/A	O-MIC-WIND-180220/420

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability'. **CVE ID : CVE-2020-0660**		
Improper Input Validation	11-02-2020	5.5	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2020-0751. **CVE ID : CVE-2020-0661**	N/A	O-MIC-WIND-180220/421
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	9	A remote code execution vulnerability exists in the way that Windows handles objects in memory, aka 'Windows Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-0662**	N/A	O-MIC-WIND-180220/422
Improper Privilege Management	11-02-2020	4	An elevation of privilege vulnerability exists when Microsoft Edge does not properly enforce cross-domain policies, which could allow an attacker to access information from one domain and inject it into another domain.In a web-based attack scenario, an attacker could host a website that is used to attempt to exploit the	N/A	O-MIC-WIND-180220/423

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, aka 'Microsoft Edge Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0663**		
Improper Privilege Management	11-02-2020	6.8	An elevation of privilege vulnerability exists in Active Directory Forest trusts due to a default setting that lets an attacker in the trusting forest request delegation of a TGT for an identity from the trusted forest, aka 'Active Directory Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0665**	N/A	O-MIC-WIND-180220/424
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0667, CVE-2020-0735, CVE-2020-0752. **CVE ID : CVE-2020-0666**	N/A	O-MIC-WIND-180220/425
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0666, CVE-2020-0735,	N/A	O-MIC-WIND-180220/426

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-0752. **CVE ID : CVE-2020-0667**		
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0669, CVE-2020-0670, CVE-2020-0671, CVE-2020-0672. **CVE ID : CVE-2020-0668**	N/A	O-MIC-WIND-180220/427
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0668, CVE-2020-0670, CVE-2020-0671, CVE-2020-0672. **CVE ID : CVE-2020-0669**	N/A	O-MIC-WIND-180220/428
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0668, CVE-2020-0669, CVE-2020-0671, CVE-2020-0672. **CVE ID : CVE-2020-0670**	N/A	O-MIC-WIND-180220/429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0668, CVE-2020-0669, CVE-2020-0670, CVE-2020-0672. **CVE ID : CVE-2020-0671**	N/A	O-MIC-WIND-180220/430
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0668, CVE-2020-0669, CVE-2020-0670, CVE-2020-0671. **CVE ID : CVE-2020-0672**	N/A	O-MIC-WIND-180220/431
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0674, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767. **CVE ID : CVE-2020-0673**	N/A	O-MIC-WIND-180220/432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767. **CVE ID : CVE-2020-0674**	N/A	O-MIC-WIND-180220/433
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0676, CVE-2020-0677, CVE-2020-0748, CVE-2020-0755, CVE-2020-0756. **CVE ID : CVE-2020-0675**	N/A	O-MIC-WIND-180220/434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0677, CVE-2020-0748, CVE-2020-0755, CVE-2020-0756. **CVE ID : CVE-2020-0676**	N/A	O-MIC-WIND-180220/435
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka	N/A	O-MIC-WIND-180220/436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0748, CVE-2020-0755, CVE-2020-0756. **CVE ID : CVE-2020-0677**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles hard links, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0678**	N/A	O-MIC-WIND-180220/437
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0680, CVE-2020-0682. **CVE ID : CVE-2020-0679**	N/A	O-MIC-WIND-180220/438
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. This CVE ID	N/A	O-MIC-WIND-180220/439

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is unique from CVE-2020-0679, CVE-2020-0682. **CVE ID : CVE-2020-0680**		
Improper Input Validation	11-02-2020	7.6	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0734. **CVE ID : CVE-2020-0681**	N/A	O-MIC-WIND-180220/440
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0679, CVE-2020-0680. **CVE ID : CVE-2020-0682**	N/A	O-MIC-WIND-180220/441
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in the Windows Installer when MSI packages process symbolic links, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0686. **CVE ID : CVE-2020-0683**	N/A	O-MIC-WIND-180220/442

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when Windows improperly handles COM object creation, aka 'Windows COM Server Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0685**	N/A	O-MIC-WIND-180220/443
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in the Windows Installer when MSI packages process symbolic links, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0683. **CVE ID : CVE-2020-0686**	N/A	O-MIC-WIND-180220/444
Improper Input Validation	11-02-2020	4.6	A security feature bypass vulnerability exists in secure boot, aka 'Microsoft Secure Boot Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-0689**	N/A	O-MIC-WIND-180220/445
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists when the Telephony Service improperly discloses the contents of its memory, aka 'Windows Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0698**	N/A	O-MIC-WIND-180220/446
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Client License Service (ClipSVC) handles objects	N/A	O-MIC-WIND-180220/447

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in memory, aka 'Windows Client License Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0701**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0703**	N/A	O-MIC-WIND-180220/448
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when the Windows Wireless Network Manager improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Wireless Network Manager Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0704**	N/A	O-MIC-WIND-180220/449
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists when the Windows Network Driver Interface Specification (NDIS) improperly handles memory.To exploit this	N/A	O-MIC-WIND-180220/450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Network Driver Interface Specification (NDIS) Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0705**		
Information Exposure	11-02-2020	4.3	An information disclosure vulnerability exists in the way that affected Microsoft browsers handle cross-origin requests, aka 'Microsoft Browser Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0706**	N/A	O-MIC-WIND-180220/451
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when the Windows IME improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows IME Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0707**	N/A	O-MIC-WIND-180220/452
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0732.	N/A	O-MIC-WIND-180220/453

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0709		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726. **CVE ID : CVE-2020-0731**	N/A	O-MIC-WIND-180220/454
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0709. **CVE ID : CVE-2020-0732**	N/A	O-MIC-WIND-180220/455
Improper Input Validation	11-02-2020	9.3	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0681.	N/A	O-MIC-WIND-180220/456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0734		
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0666, CVE-2020-0667, CVE-2020-0752. **CVE ID : CVE-2020-0735**	N/A	O-MIC-WIND-180220/457
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the tapisrv.dll handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0739. **CVE ID : CVE-2020-0737**	N/A	O-MIC-WIND-180220/458
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	9.3	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. **CVE ID : CVE-2020-0738**	N/A	O-MIC-WIND-180220/459
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the dssvc.dll handles file creation allowing for a file overwrite or creation in a secured location, aka	N/A	O-MIC-WIND-180220/460

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0737. **CVE ID : CVE-2020-0739**		
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0741, CVE-2020-0742, CVE-2020-0743, CVE-2020-0749, CVE-2020-0750. **CVE ID : CVE-2020-0740**	N/A	O-MIC-WIND-180220/461
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0740, CVE-2020-0742, CVE-2020-0743, CVE-2020-0749, CVE-2020-0750. **CVE ID : CVE-2020-0741**	N/A	O-MIC-WIND-180220/462
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service	N/A	O-MIC-WIND-180220/463

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0740, CVE-2020-0741, CVE-2020-0743, CVE-2020-0749, CVE-2020-0750. **CVE ID : CVE-2020-0742**		
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0740, CVE-2020-0741, CVE-2020-0742, CVE-2020-0749, CVE-2020-0750. **CVE ID : CVE-2020-0743**	N/A	O-MIC-WIND-180220/464
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an attacker to retrieve information from a targeted system, aka 'Windows GDI Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0744**	N/A	O-MIC-WIND-180220/465
Improper	11-02-2020	7.2	An elevation of privilege	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0715, CVE-2020-0792. **CVE ID : CVE-2020-0745**		180220/466
Information Exposure	11-02-2020	5	An information disclosure vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0746**	N/A	O-MIC-WIND-180220/467
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka 'Windows Data Sharing Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0659. **CVE ID : CVE-2020-0747**	N/A	O-MIC-WIND-180220/468
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker	N/A	O-MIC-WIND-180220/469

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0677, CVE-2020-0755, CVE-2020-0756. **CVE ID : CVE-2020-0748**		
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0740, CVE-2020-0741, CVE-2020-0742, CVE-2020-0743, CVE-2020-0750. **CVE ID : CVE-2020-0749**	N/A	O-MIC-WIND-180220/470
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege	N/A	O-MIC-WIND-180220/471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. This CVE ID is unique from CVE-2020-0740, CVE-2020-0741, CVE-2020-0742, CVE-2020-0743, CVE-2020-0749. **CVE ID : CVE-2020-0750**		
Improper Input Validation	11-02-2020	2.1	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate specific malicious data from a user on a guest operating system.To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application.The security update addresses the vulnerability by resolving the conditions where Hyper-V would fail to handle these requests., aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2020-0661. **CVE ID : CVE-2020-0751**	N/A	O-MIC-WIND-180220/472
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege	N/A	O-MIC-WIND-180220/473

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. This CVE ID is unique from CVE-2020-0666, CVE-2020-0667, CVE-2020-0735. **CVE ID : CVE-2020-0752**		
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0754. **CVE ID : CVE-2020-0753**	N/A	O-MIC-WIND-180220/474
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0753. **CVE ID : CVE-2020-0754**	N/A	O-MIC-WIND-180220/475
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security	N/A	O-MIC-WIND-180220/476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0677, CVE-2020-0748, CVE-2020-0756. **CVE ID : CVE-2020-0755**		
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0677, CVE-2020-0748, CVE-2020-0755. **CVE ID : CVE-2020-0756**	N/A	O-MIC-WIND-180220/477
Improper Privilege	11-02-2020	7.2	An elevation of privilege vulnerability exists when	N/A	O-MIC-WIND-180220/478

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Windows improperly handles Secure Socket Shell remote commands, aka 'Windows SSH Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0757**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713. **CVE ID : CVE-2020-0767**	N/A	O-MIC-WIND-180220/479
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0715, CVE-2020-0745. **CVE ID : CVE-2020-0792**	N/A	O-MIC-WIND-180220/480
windows_7					
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in	N/A	O-MIC-WIND-180220/481

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0719**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0720**	N/A	O-MIC-WIND-180220/482
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-	N/A	O-MIC-WIND-180220/483

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0721**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0722**	N/A	O-MIC-WIND-180220/484
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731.	N/A	O-MIC-WIND-180220/485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0723		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0724**	N/A	O-MIC-WIND-180220/486
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0725**	N/A	O-MIC-WIND-180220/487
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in	N/A	O-MIC-WIND-180220/488

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0731. **CVE ID : CVE-2020-0726**		
N/A	11-02-2020	6.8	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-0729**	N/A	O-MIC-WIND-180220/489
Improper Link Resolution Before File Access ('Link Following')	11-02-2020	3.6	An elevation of privilege vulnerability exists when the Windows User Profile Service (ProfSvc) improperly handles symlinks, aka 'Windows User Profile Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0730**	N/A	O-MIC-WIND-180220/490
Improper Input Validation	11-02-2020	8.5	A remote code execution vulnerability exists in Remote Desktop Services â€“ formerly known as	N/A	O-MIC-WIND-180220/491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Terminal Services â€“ when an authenticated attacker abuses clipboard redirection, aka 'Remote Desktop ServicesÂ Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-0655**		
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory, aka 'Windows Common Log File System Driver Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0657**	N/A	O-MIC-WIND-180220/492
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists in the Windows Common Log File System (CLFS) driver when it fails to properly handle objects in memory, aka 'Windows Common Log File System Driver Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0658**	N/A	O-MIC-WIND-180220/493
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	9	A remote code execution vulnerability exists in the way that Windows handles objects in memory, aka 'Windows Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-0662**	N/A	O-MIC-WIND-180220/494
Improper	11-02-2020	6.8	An elevation of privilege	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			vulnerability exists in Active Directory Forest trusts due to a default setting that lets an attacker in the trusting forest request delegation of a TGT for an identity from the trusted forest, aka 'Active Directory Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0665**		180220/495
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0667, CVE-2020-0735, CVE-2020-0752. **CVE ID : CVE-2020-0666**	N/A	O-MIC-WIND-180220/496
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0666, CVE-2020-0735, CVE-2020-0752. **CVE ID : CVE-2020-0667**	N/A	O-MIC-WIND-180220/497
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows	N/A	O-MIC-WIND-180220/498

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0669, CVE-2020-0670, CVE-2020-0671, CVE-2020-0672. **CVE ID : CVE-2020-0668**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0674, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767. **CVE ID : CVE-2020-0673**	N/A	O-MIC-WIND-180220/499
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767. **CVE ID : CVE-2020-0674**	N/A	O-MIC-WIND-180220/500

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0676, CVE-2020-0677, CVE-2020-0748, CVE-2020-0755, CVE-2020-0756. **CVE ID : CVE-2020-0675**	N/A	O-MIC-WIND-180220/501
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka	N/A	O-MIC-WIND-180220/502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0677, CVE-2020-0748, CVE-2020-0755, CVE-2020-0756. **CVE ID : CVE-2020-0676**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0748, CVE-2020-0755, CVE-2020-0756. **CVE ID : CVE-2020-0677**	N/A	O-MIC-WIND-180220/503
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles hard links, aka 'Windows Error Reporting	N/A	O-MIC-WIND-180220/504

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Manager Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0678**		
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0680, CVE-2020-0682. **CVE ID : CVE-2020-0679**	N/A	O-MIC-WIND-180220/505
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0679, CVE-2020-0682. **CVE ID : CVE-2020-0680**	N/A	O-MIC-WIND-180220/506
Improper Input Validation	11-02-2020	7.6	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0734. **CVE ID : CVE-2020-0681**	N/A	O-MIC-WIND-180220/507

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0679, CVE-2020-0680. **CVE ID : CVE-2020-0682**	N/A	O-MIC-WIND-180220/508
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in the Windows Installer when MSI packages process symbolic links, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0686. **CVE ID : CVE-2020-0683**	N/A	O-MIC-WIND-180220/509
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in the Windows Installer when MSI packages process symbolic links, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0683. **CVE ID : CVE-2020-0686**	N/A	O-MIC-WIND-180220/510
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists when the Telephony Service improperly discloses the contents of its memory,	N/A	O-MIC-WIND-180220/511

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			aka 'Windows Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0698**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0703**	N/A	O-MIC-WIND-180220/512
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists when the Windows Network Driver Interface Specification (NDIS) improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Network Driver Interface Specification (NDIS) Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0705**	N/A	O-MIC-WIND-180220/513
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege	N/A	O-MIC-WIND-180220/514

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726. **CVE ID : CVE-2020-0731**		
Improper Input Validation	11-02-2020	9.3	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0681. **CVE ID : CVE-2020-0734**	N/A	O-MIC-WIND-180220/515
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0666, CVE-2020-0667, CVE-2020-0752. **CVE ID : CVE-2020-0735**	N/A	O-MIC-WIND-180220/516
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka	N/A	O-MIC-WIND-180220/517

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			'Windows Kernel Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0736**		
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the tapisrv.dll handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0739. **CVE ID : CVE-2020-0737**	N/A	O-MIC-WIND-180220/518
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	9.3	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. **CVE ID : CVE-2020-0738**	N/A	O-MIC-WIND-180220/519
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an attacker to retrieve information from a targeted system, aka 'Windows GDI Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0744**	N/A	O-MIC-WIND-180220/520
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly	N/A	O-MIC-WIND-180220/521

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0715, CVE-2020-0792. **CVE ID : CVE-2020-0745**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0677, CVE-2020-0755, CVE-2020-0756. **CVE ID : CVE-2020-0748**	N/A	O-MIC-WIND-180220/522
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege	N/A	O-MIC-WIND-180220/523

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. This CVE ID is unique from CVE-2020-0666, CVE-2020-0667, CVE-2020-0735. **CVE ID : CVE-2020-0752**		
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0754. **CVE ID : CVE-2020-0753**	N/A	O-MIC-WIND-180220/524
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0753. **CVE ID : CVE-2020-0754**	N/A	O-MIC-WIND-180220/525
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security	N/A	O-MIC-WIND-180220/526

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0677, CVE-2020-0748, CVE-2020-0756. **CVE ID : CVE-2020-0755**		
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0677, CVE-2020-0748, CVE-2020-0755. **CVE ID : CVE-2020-0756**	N/A	O-MIC-WIND-180220/527
windows_8.1					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0717. **CVE ID : CVE-2020-0716**	N/A	O-MIC-WIND-180220/528
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0719**	N/A	O-MIC-WIND-180220/529
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724,	N/A	O-MIC-WIND-180220/530

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0720**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0721**	N/A	O-MIC-WIND-180220/531
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0722**	N/A	O-MIC-WIND-180220/532
Improper	11-02-2020	7.2	An elevation of privilege	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0723**		180220/533
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0724**	N/A	O-MIC-WIND-180220/534
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege	N/A	O-MIC-WIND-180220/535

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0725**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0731. **CVE ID : CVE-2020-0726**	N/A	O-MIC-WIND-180220/536
N/A	11-02-2020	6.8	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'.	N/A	O-MIC-WIND-180220/537

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0729		
Improper Link Resolution Before File Access ('Link Following')	11-02-2020	3.6	An elevation of privilege vulnerability exists when the Windows User Profile Service (ProfSvc) improperly handles symlinks, aka 'Windows User Profile Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0730**	N/A	O-MIC-WIND-180220/538
Improper Input Validation	11-02-2020	8.5	A remote code execution vulnerability exists in Remote Desktop Services â€“ formerly known as Terminal Services â€“ when an authenticated attacker abuses clipboard redirection, aka 'Remote Desktop ServicesÂ Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-0655**	N/A	O-MIC-WIND-180220/539
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory, aka 'Windows Common Log File System Driver Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0657**	N/A	O-MIC-WIND-180220/540
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists in the Windows Common Log File System (CLFS) driver when it fails to properly	N/A	O-MIC-WIND-180220/541

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			handle objects in memory, aka 'Windows Common Log File System Driver Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0658**		
Improper Input Validation	11-02-2020	5	A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability'. **CVE ID : CVE-2020-0660**	N/A	O-MIC-WIND-180220/542
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	9	A remote code execution vulnerability exists in the way that Windows handles objects in memory, aka 'Windows Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-0662**	N/A	O-MIC-WIND-180220/543
Improper Privilege Management	11-02-2020	6.8	An elevation of privilege vulnerability exists in Active Directory Forest trusts due to a default setting that lets an attacker in the trusting forest request delegation of a TGT for an identity from the trusted forest, aka 'Active Directory Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0665**	N/A	O-MIC-WIND-180220/544

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0667, CVE-2020-0735, CVE-2020-0752. **CVE ID : CVE-2020-0666**	N/A	O-MIC-WIND-180220/545
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0666, CVE-2020-0735, CVE-2020-0752. **CVE ID : CVE-2020-0667**	N/A	O-MIC-WIND-180220/546
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0669, CVE-2020-0670, CVE-2020-0671, CVE-2020-0672. **CVE ID : CVE-2020-0668**	N/A	O-MIC-WIND-180220/547
Improper Restriction of	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the scripting	N/A	O-MIC-WIND-180220/548

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0674, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767. **CVE ID : CVE-2020-0673**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767. **CVE ID : CVE-2020-0674**	N/A	O-MIC-WIND-180220/549
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the	N/A	O-MIC-WIND-180220/550

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0676, CVE-2020-0677, CVE-2020-0748, CVE-2020-0755, CVE-2020-0756. **CVE ID : CVE-2020-0675**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0677, CVE-2020-0748, CVE-2020-0755, CVE-2020-0756. **CVE ID : CVE-2020-0676**	N/A	O-MIC-WIND-180220/551
Improper Restriction of	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next	N/A	O-MIC-WIND-180220/552

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0748, CVE-2020-0755, CVE-2020-0756. **CVE ID : CVE-2020-0677**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles hard links, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0678**	N/A	O-MIC-WIND-180220/553
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. This CVE ID	N/A	O-MIC-WIND-180220/554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is unique from CVE-2020-0680, CVE-2020-0682. **CVE ID : CVE-2020-0679**		
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0679, CVE-2020-0682. **CVE ID : CVE-2020-0680**	N/A	O-MIC-WIND-180220/555
Improper Input Validation	11-02-2020	7.6	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0734. **CVE ID : CVE-2020-0681**	N/A	O-MIC-WIND-180220/556
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0679, CVE-2020-0680. **CVE ID : CVE-2020-0682**	N/A	O-MIC-WIND-180220/557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in the Windows Installer when MSI packages process symbolic links, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0686. **CVE ID : CVE-2020-0683**	N/A	O-MIC-WIND-180220/558
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in the Windows Installer when MSI packages process symbolic links, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0683. **CVE ID : CVE-2020-0686**	N/A	O-MIC-WIND-180220/559
Improper Input Validation	11-02-2020	4.6	A security feature bypass vulnerability exists in secure boot, aka 'Microsoft Secure Boot Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-0689**	N/A	O-MIC-WIND-180220/560
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists when the Telephony Service improperly discloses the contents of its memory, aka 'Windows Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0698**	N/A	O-MIC-WIND-180220/561
Information	11-02-2020	2.1	An information disclosure vulnerability exists when	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			the Windows Network Driver Interface Specification (NDIS) improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Network Driver Interface Specification (NDIS) Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0705**		180220/562
Information Exposure	11-02-2020	4.3	An information disclosure vulnerability exists in the way that affected Microsoft browsers handle cross-origin requests, aka 'Microsoft Browser Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0706**	N/A	O-MIC-WIND-180220/563
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when the Windows IME improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows IME Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0707**	N/A	O-MIC-WIND-180220/564
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to	N/A	O-MIC-WIND-180220/565

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726. **CVE ID : CVE-2020-0731**		
Improper Input Validation	11-02-2020	9.3	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0681. **CVE ID : CVE-2020-0734**	N/A	O-MIC-WIND-180220/566
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0666, CVE-2020-0667, CVE-2020-0752. **CVE ID : CVE-2020-0735**	N/A	O-MIC-WIND-180220/567
Improper Privilege	11-02-2020	4.6	An elevation of privilege vulnerability exists in the	N/A	O-MIC-WIND-180220/568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			way that the tapisrv.dll handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0739. **CVE ID : CVE-2020-0737**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	9.3	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. **CVE ID : CVE-2020-0738**	N/A	O-MIC-WIND-180220/569
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an attacker to retrieve information from a targeted system, aka 'Windows GDI Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0744**	N/A	O-MIC-WIND-180220/570
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-	N/A	O-MIC-WIND-180220/571

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0715, CVE-2020-0792. **CVE ID : CVE-2020-0745**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0677, CVE-2020-0755, CVE-2020-0756. **CVE ID : CVE-2020-0748**	N/A	O-MIC-WIND-180220/572
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0666, CVE-2020-0667, CVE-2020-0735. **CVE ID : CVE-2020-0752**	N/A	O-MIC-WIND-180220/573

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0754. **CVE ID : CVE-2020-0753**	N/A	O-MIC-WIND-180220/574
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0753. **CVE ID : CVE-2020-0754**	N/A	O-MIC-WIND-180220/575
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information	N/A	O-MIC-WIND-180220/576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0677, CVE-2020-0748, CVE-2020-0756. **CVE ID : CVE-2020-0755**		
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0677, CVE-2020-0748, CVE-2020-0755. **CVE ID : CVE-2020-0756**	N/A	O-MIC-WIND-180220/577
windows_rt_8.1					
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'.	N/A	O-MIC-WIND-180220/578

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This CVE ID is unique from CVE-2020-0717. **CVE ID : CVE-2020-0716**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0719**	N/A	O-MIC-WIND-180220/579
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0720**	N/A	O-MIC-WIND-180220/580
Improper Privilege	11-02-2020	7.2	An elevation of privilege vulnerability exists in	N/A	O-MIC-WIND-180220/581

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0721**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0722**	N/A	O-MIC-WIND-180220/582
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID	N/A	O-MIC-WIND-180220/583

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0723**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0724**	N/A	O-MIC-WIND-180220/584
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-	N/A	O-MIC-WIND-180220/585

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0725**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0731. **CVE ID : CVE-2020-0726**	N/A	O-MIC-WIND-180220/586
N/A	11-02-2020	6.8	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-0729**	N/A	O-MIC-WIND-180220/587
Improper Link Resolution Before File Access ('Link Following')	11-02-2020	3.6	An elevation of privilege vulnerability exists when the Windows User Profile Service (ProfSvc) improperly handles symlinks, aka 'Windows	N/A	O-MIC-WIND-180220/588

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			User Profile Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0730**		
Improper Input Validation	11-02-2020	8.5	A remote code execution vulnerability exists in Remote Desktop Services â€“ formerly known as Terminal Services â€“ when an authenticated attacker abuses clipboard redirection, aka 'Remote Desktop ServicesÂ Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-0655**	N/A	O-MIC-WIND-180220/589
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory, aka 'Windows Common Log File System Driver Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0657**	N/A	O-MIC-WIND-180220/590
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists in the Windows Common Log File System (CLFS) driver when it fails to properly handle objects in memory, aka 'Windows Common Log File System Driver Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0658**	N/A	O-MIC-WIND-180220/591

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	11-02-2020	5	A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability'. **CVE ID : CVE-2020-0660**	N/A	O-MIC-WIND-180220/592
Improper Privilege Management	11-02-2020	6.8	An elevation of privilege vulnerability exists in Active Directory Forest trusts due to a default setting that lets an attacker in the trusting forest request delegation of a TGT for an identity from the trusted forest, aka 'Active Directory Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0665**	N/A	O-MIC-WIND-180220/593
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0667, CVE-2020-0735, CVE-2020-0752. **CVE ID : CVE-2020-0666**	N/A	O-MIC-WIND-180220/594
Improper Privilege	11-02-2020	4.6	An elevation of privilege vulnerability exists in the	N/A	O-MIC-WIND-180220/595

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0666, CVE-2020-0735, CVE-2020-0752. **CVE ID : CVE-2020-0667**		
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0669, CVE-2020-0670, CVE-2020-0671, CVE-2020-0672. **CVE ID : CVE-2020-0668**	N/A	O-MIC-WIND-180220/596
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0674, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767. **CVE ID : CVE-2020-0673**	N/A	O-MIC-WIND-180220/597
Improper Restriction	11-02-2020	7.6	A remote code execution vulnerability exists in the	N/A	O-MIC-WIND-180220/598

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767. **CVE ID : CVE-2020-0674**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0676, CVE-2020-0677, CVE-2020-0748, CVE-2020-0755, CVE-2020-0756. **CVE ID : CVE-2020-0675**	N/A	O-MIC-WIND-180220/599
Improper Restriction	11-02-2020	2.1	An information disclosure vulnerability exists in the	N/A	O-MIC-WIND-180220/600

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0677, CVE-2020-0748, CVE-2020-0755, CVE-2020-0756. **CVE ID : CVE-2020-0676**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information	N/A	O-MIC-WIND-180220/601

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0748, CVE-2020-0755, CVE-2020-0756. **CVE ID : CVE-2020-0677**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles hard links, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0678**	N/A	O-MIC-WIND-180220/602
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0680, CVE-2020-0682. **CVE ID : CVE-2020-0679**	N/A	O-MIC-WIND-180220/603
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0679, CVE-2020-0682.	N/A	O-MIC-WIND-180220/604

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0680		
Improper Input Validation	11-02-2020	7.6	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0734. **CVE ID : CVE-2020-0681**	N/A	O-MIC-WIND-180220/605
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0679, CVE-2020-0680. **CVE ID : CVE-2020-0682**	N/A	O-MIC-WIND-180220/606
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in the Windows Installer when MSI packages process symbolic links, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0686. **CVE ID : CVE-2020-0683**	N/A	O-MIC-WIND-180220/607
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in the Windows Installer when	N/A	O-MIC-WIND-180220/608

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSI packages process symbolic links, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0683. **CVE ID : CVE-2020-0686**		
Improper Input Validation	11-02-2020	4.6	A security feature bypass vulnerability exists in secure boot, aka 'Microsoft Secure Boot Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-0689**	N/A	O-MIC-WIND-180220/609
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists when the Telephony Service improperly discloses the contents of its memory, aka 'Windows Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0698**	N/A	O-MIC-WIND-180220/610
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists when the Windows Network Driver Interface Specification (NDIS) improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Network Driver Interface Specification (NDIS) Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0705**	N/A	O-MIC-WIND-180220/611

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	11-02-2020	4.3	An information disclosure vulnerability exists in the way that affected Microsoft browsers handle cross-origin requests, aka 'Microsoft Browser Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0706**	N/A	O-MIC-WIND-180220/612
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when the Windows IME improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows IME Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0707**	N/A	O-MIC-WIND-180220/613
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726. **CVE ID : CVE-2020-0731**	N/A	O-MIC-WIND-180220/614
Improper	11-02-2020	9.3	A remote code execution	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0681. **CVE ID : CVE-2020-0734**		180220/615
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0666, CVE-2020-0667, CVE-2020-0752. **CVE ID : CVE-2020-0735**	N/A	O-MIC-WIND-180220/616
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the tapisrv.dll handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0739. **CVE ID : CVE-2020-0737**	N/A	O-MIC-WIND-180220/617
Improper Restriction of Operations within the Bounds of a	11-02-2020	9.3	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media	N/A	O-MIC-WIND-180220/618

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Foundation Memory Corruption Vulnerability'. **CVE ID : CVE-2020-0738**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an attacker to retrieve information from a targeted system, aka 'Windows GDI Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0744**	N/A	O-MIC-WIND-180220/619
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0715, CVE-2020-0792. **CVE ID : CVE-2020-0745**	N/A	O-MIC-WIND-180220/620
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security	N/A	O-MIC-WIND-180220/621

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0677, CVE-2020-0755, CVE-2020-0756. **CVE ID : CVE-2020-0748**		
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0666, CVE-2020-0667, CVE-2020-0735. **CVE ID : CVE-2020-0752**	N/A	O-MIC-WIND-180220/622
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0754. **CVE ID : CVE-2020-0753**	N/A	O-MIC-WIND-180220/623
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in Windows Error Reporting	N/A	O-MIC-WIND-180220/624

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0753. **CVE ID : CVE-2020-0754**		
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0677, CVE-2020-0748, CVE-2020-0756. **CVE ID : CVE-2020-0755**	N/A	O-MIC-WIND-180220/625
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this	N/A	O-MIC-WIND-180220/626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0677, CVE-2020-0748, CVE-2020-0755. **CVE ID : CVE-2020-0756**		
windows_server_2008					
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0719**	N/A	O-MIC-WIND-180220/627
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to	N/A	O-MIC-WIND-180220/628

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0720**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0721**	N/A	O-MIC-WIND-180220/629
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719,	N/A	O-MIC-WIND-180220/630

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-0720, CVE-2020-0721, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0722**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0723**	N/A	O-MIC-WIND-180220/631
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731.	N/A	O-MIC-WIND-180220/632

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0724		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0725**	N/A	O-MIC-WIND-180220/633
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0731. **CVE ID : CVE-2020-0726**	N/A	O-MIC-WIND-180220/634
N/A	11-02-2020	6.8	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is	N/A	O-MIC-WIND-180220/635

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-0729**		
Improper Link Resolution Before File Access ('Link Following')	11-02-2020	3.6	An elevation of privilege vulnerability exists when the Windows User Profile Service (ProfSvc) improperly handles symlinks, aka 'Windows User Profile Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0730**	N/A	O-MIC-WIND-180220/636
Improper Input Validation	11-02-2020	8.5	A remote code execution vulnerability exists in Remote Desktop Services â€“ formerly known as Terminal Services â€“ when an authenticated attacker abuses clipboard redirection, aka 'Remote Desktop ServicesÂ Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-0655**	N/A	O-MIC-WIND-180220/637
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory, aka 'Windows Common Log File System Driver Elevation of Privilege	N/A	O-MIC-WIND-180220/638

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. **CVE ID : CVE-2020-0657**		
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists in the Windows Common Log File System (CLFS) driver when it fails to properly handle objects in memory, aka 'Windows Common Log File System Driver Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0658**	N/A	O-MIC-WIND-180220/639
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	9	A remote code execution vulnerability exists in the way that Windows handles objects in memory, aka 'Windows Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-0662**	N/A	O-MIC-WIND-180220/640
Improper Privilege Management	11-02-2020	6.8	An elevation of privilege vulnerability exists in Active Directory Forest trusts due to a default setting that lets an attacker in the trusting forest request delegation of a TGT for an identity from the trusted forest, aka 'Active Directory Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0665**	N/A	O-MIC-WIND-180220/641
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka	N/A	O-MIC-WIND-180220/642

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0667, CVE-2020-0735, CVE-2020-0752. **CVE ID : CVE-2020-0666**		
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0666, CVE-2020-0735, CVE-2020-0752. **CVE ID : CVE-2020-0667**	N/A	O-MIC-WIND-180220/643
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0669, CVE-2020-0670, CVE-2020-0671, CVE-2020-0672. **CVE ID : CVE-2020-0668**	N/A	O-MIC-WIND-180220/644
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'.	N/A	O-MIC-WIND-180220/645

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This CVE ID is unique from CVE-2020-0674, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767. **CVE ID : CVE-2020-0673**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767. **CVE ID : CVE-2020-0674**	N/A	O-MIC-WIND-180220/646
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information	N/A	O-MIC-WIND-180220/647

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0676, CVE-2020-0677, CVE-2020-0748, CVE-2020-0755, CVE-2020-0756. **CVE ID : CVE-2020-0675**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0677, CVE-2020-0748, CVE-2020-0755, CVE-2020-0756. **CVE ID : CVE-2020-0676**	N/A	O-MIC-WIND-180220/648
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker	N/A	O-MIC-WIND-180220/649

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0748, CVE-2020-0755, CVE-2020-0756. **CVE ID : CVE-2020-0677**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles hard links, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0678**	N/A	O-MIC-WIND-180220/650
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0679, CVE-2020-0682. **CVE ID : CVE-2020-0680**	N/A	O-MIC-WIND-180220/651
Improper	11-02-2020	7.6	A remote code execution	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0734. **CVE ID : CVE-2020-0681**		180220/652
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0679, CVE-2020-0680. **CVE ID : CVE-2020-0682**	N/A	O-MIC-WIND-180220/653
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in the Windows Installer when MSI packages process symbolic links, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0686. **CVE ID : CVE-2020-0683**	N/A	O-MIC-WIND-180220/654
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in the Windows Installer when MSI packages process symbolic links, aka	N/A	O-MIC-WIND-180220/655

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0683. **CVE ID : CVE-2020-0686**		
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists when the Telephony Service improperly discloses the contents of its memory, aka 'Windows Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0698**	N/A	O-MIC-WIND-180220/656
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0703**	N/A	O-MIC-WIND-180220/657
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists when the Windows Network Driver Interface Specification (NDIS) improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Network Driver Interface	N/A	O-MIC-WIND-180220/658

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Specification (NDIS) Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0705**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726. **CVE ID : CVE-2020-0731**	N/A	O-MIC-WIND-180220/659
Improper Input Validation	11-02-2020	9.3	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0681. **CVE ID : CVE-2020-0734**	N/A	O-MIC-WIND-180220/660
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer	N/A	O-MIC-WIND-180220/661

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0666, CVE-2020-0667, CVE-2020-0752. **CVE ID : CVE-2020-0735**		
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0736**	N/A	O-MIC-WIND-180220/662
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the tapisrv.dll handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0739. **CVE ID : CVE-2020-0737**	N/A	O-MIC-WIND-180220/663
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	9.3	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. **CVE ID : CVE-2020-0738**	N/A	O-MIC-WIND-180220/664
Improper Restriction of Operations within the	11-02-2020	2.1	An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in	N/A	O-MIC-WIND-180220/665

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			memory, allowing an attacker to retrieve information from a targeted system, aka 'Windows GDI Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0744**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0715, CVE-2020-0792. **CVE ID : CVE-2020-0745**	N/A	O-MIC-WIND-180220/666
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-	N/A	O-MIC-WIND-180220/667

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-0676, CVE-2020-0677, CVE-2020-0755, CVE-2020-0756. **CVE ID : CVE-2020-0748**		
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0666, CVE-2020-0667, CVE-2020-0735. **CVE ID : CVE-2020-0752**	N/A	O-MIC-WIND-180220/668
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0754. **CVE ID : CVE-2020-0753**	N/A	O-MIC-WIND-180220/669
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0753. **CVE ID : CVE-2020-0754**	N/A	O-MIC-WIND-180220/670

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0677, CVE-2020-0748, CVE-2020-0756. **CVE ID : CVE-2020-0755**	N/A	O-MIC-WIND-180220/671
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka	N/A	O-MIC-WIND-180220/672

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0677, CVE-2020-0748, CVE-2020-0755. **CVE ID : CVE-2020-0756**		
windows_server_2012					
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0717. **CVE ID : CVE-2020-0716**	N/A	O-MIC-WIND-180220/673
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0719**	N/A	O-MIC-WIND-180220/674
Improper Privilege	11-02-2020	7.2	An elevation of privilege vulnerability exists in	N/A	O-MIC-WIND-180220/675

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0720**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0721**	N/A	O-MIC-WIND-180220/676
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID	N/A	O-MIC-WIND-180220/677

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0722**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0723**	N/A	O-MIC-WIND-180220/678
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0725, CVE-	N/A	O-MIC-WIND-180220/679

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0724**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0725**	N/A	O-MIC-WIND-180220/680
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0731. **CVE ID : CVE-2020-0726**	N/A	O-MIC-WIND-180220/681
N/A	11-02-2020	6.8	A remote code execution vulnerability exists in	N/A	O-MIC-WIND-180220/682

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-0729**		
Improper Link Resolution Before File Access ('Link Following')	11-02-2020	3.6	An elevation of privilege vulnerability exists when the Windows User Profile Service (ProfSvc) improperly handles symlinks, aka 'Windows User Profile Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0730**	N/A	O-MIC-WIND-180220/683
Improper Input Validation	11-02-2020	8.5	A remote code execution vulnerability exists in Remote Desktop Services â€“ formerly known as Terminal Services â€“ when an authenticated attacker abuses clipboard redirection, aka 'Remote Desktop ServicesÂ Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-0655**	N/A	O-MIC-WIND-180220/684
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory, aka	N/A	O-MIC-WIND-180220/685

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			'Windows Common Log File System Driver Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0657**		
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists in the Windows Common Log File System (CLFS) driver when it fails to properly handle objects in memory, aka 'Windows Common Log File System Driver Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0658**	N/A	O-MIC-WIND-180220/686
Improper Input Validation	11-02-2020	5	A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability'. **CVE ID : CVE-2020-0660**	N/A	O-MIC-WIND-180220/687
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	9	A remote code execution vulnerability exists in the way that Windows handles objects in memory, aka 'Windows Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-0662**	N/A	O-MIC-WIND-180220/688
Improper Privilege Management	11-02-2020	6.8	An elevation of privilege vulnerability exists in Active Directory Forest	N/A	O-MIC-WIND-180220/689

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			trusts due to a default setting that lets an attacker in the trusting forest request delegation of a TGT for an identity from the trusted forest, aka 'Active Directory Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0665**		
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0667, CVE-2020-0735, CVE-2020-0752. **CVE ID : CVE-2020-0666**	N/A	O-MIC-WIND-180220/690
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0666, CVE-2020-0735, CVE-2020-0752. **CVE ID : CVE-2020-0667**	N/A	O-MIC-WIND-180220/691
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows	N/A	O-MIC-WIND-180220/692

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0669, CVE-2020-0670, CVE-2020-0671, CVE-2020-0672. **CVE ID : CVE-2020-0668**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0674, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767. **CVE ID : CVE-2020-0673**	N/A	O-MIC-WIND-180220/693
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767. **CVE ID : CVE-2020-0674**	N/A	O-MIC-WIND-180220/694
Improper Restriction	11-02-2020	2.1	An information disclosure vulnerability exists in the	N/A	O-MIC-WIND-180220/695

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0676, CVE-2020-0677, CVE-2020-0748, CVE-2020-0755, CVE-2020-0756. **CVE ID : CVE-2020-0675**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information	N/A	O-MIC-WIND-180220/696

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0677, CVE-2020-0748, CVE-2020-0755, CVE-2020-0756. **CVE ID : CVE-2020-0676**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0748, CVE-2020-0755, CVE-2020-0756. **CVE ID : CVE-2020-0677**	N/A	O-MIC-WIND-180220/697
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles hard links, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'.	N/A	O-MIC-WIND-180220/698

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0678		
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0680, CVE-2020-0682. **CVE ID : CVE-2020-0679**	N/A	O-MIC-WIND-180220/699
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0679, CVE-2020-0682. **CVE ID : CVE-2020-0680**	N/A	O-MIC-WIND-180220/700
Improper Input Validation	11-02-2020	7.6	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0734. **CVE ID : CVE-2020-0681**	N/A	O-MIC-WIND-180220/701
Improper Privilege	11-02-2020	7.2	An elevation of privilege vulnerability exists in the	N/A	O-MIC-WIND-180220/702

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0679, CVE-2020-0680. **CVE ID : CVE-2020-0682**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in the Windows Installer when MSI packages process symbolic links, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0686. **CVE ID : CVE-2020-0683**	N/A	O-MIC-WIND-180220/703
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in the Windows Installer when MSI packages process symbolic links, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0683. **CVE ID : CVE-2020-0686**	N/A	O-MIC-WIND-180220/704
Improper Input Validation	11-02-2020	4.6	A security feature bypass vulnerability exists in secure boot, aka 'Microsoft Secure Boot Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-0689**	N/A	O-MIC-WIND-180220/705

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists when the Telephony Service improperly discloses the contents of its memory, aka 'Windows Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0698**	N/A	O-MIC-WIND-180220/706
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0703**	N/A	O-MIC-WIND-180220/707
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists when the Windows Network Driver Interface Specification (NDIS) improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Network Driver Interface Specification (NDIS) Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0705**	N/A	O-MIC-WIND-180220/708
Information Exposure	11-02-2020	4.3	An information disclosure vulnerability exists in the	N/A	O-MIC-WIND-180220/709

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			way that affected Microsoft browsers handle cross-origin requests, aka 'Microsoft Browser Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0706**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when the Windows IME improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows IME Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0707**	N/A	O-MIC-WIND-180220/710
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726. **CVE ID : CVE-2020-0731**	N/A	O-MIC-WIND-180220/711
Improper Input Validation	11-02-2020	9.3	A remote code execution vulnerability exists in the Windows Remote Desktop	N/A	O-MIC-WIND-180220/712

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0681. **CVE ID : CVE-2020-0734**		
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0666, CVE-2020-0667, CVE-2020-0752. **CVE ID : CVE-2020-0735**	N/A	O-MIC-WIND-180220/713
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the tapisrv.dll handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0739. **CVE ID : CVE-2020-0737**	N/A	O-MIC-WIND-180220/714
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	9.3	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'.	N/A	O-MIC-WIND-180220/715

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0738		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an attacker to retrieve information from a targeted system, aka 'Windows GDI Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0744**	N/A	O-MIC-WIND-180220/716
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0715, CVE-2020-0792. **CVE ID : CVE-2020-0745**	N/A	O-MIC-WIND-180220/717
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles	N/A	O-MIC-WIND-180220/718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0677, CVE-2020-0755, CVE-2020-0756. **CVE ID : CVE-2020-0748**		
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0666, CVE-2020-0667, CVE-2020-0735. **CVE ID : CVE-2020-0752**	N/A	O-MIC-WIND-180220/719
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0754. **CVE ID : CVE-2020-0753**	N/A	O-MIC-WIND-180220/720
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting	N/A	O-MIC-WIND-180220/721

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0753. **CVE ID : CVE-2020-0754**		
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0677, CVE-2020-0748, CVE-2020-0756. **CVE ID : CVE-2020-0755**	N/A	O-MIC-WIND-180220/722
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a	N/A	O-MIC-WIND-180220/723

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0677, CVE-2020-0748, CVE-2020-0755. **CVE ID : CVE-2020-0756**		
windows_server_2016					
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767. **CVE ID : CVE-2020-0710**	N/A	O-MIC-WIND-180220/724
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-	N/A	O-MIC-WIND-180220/725

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0710, CVE-2020-0711, CVE-2020-0713, CVE-2020-0767. **CVE ID : CVE-2020-0712**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0767. **CVE ID : CVE-2020-0713**	N/A	O-MIC-WIND-180220/726
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0717. **CVE ID : CVE-2020-0716**	N/A	O-MIC-WIND-180220/727
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0716. **CVE ID : CVE-2020-0717**	N/A	O-MIC-WIND-180220/728

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0719**	N/A	O-MIC-WIND-180220/729
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0720**	N/A	O-MIC-WIND-180220/730
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k	N/A	O-MIC-WIND-180220/731

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0721**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0722**	N/A	O-MIC-WIND-180220/732
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-	N/A	O-MIC-WIND-180220/733

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0722, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0723**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0724**	N/A	O-MIC-WIND-180220/734
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0725**	N/A	O-MIC-WIND-180220/735

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0731. **CVE ID : CVE-2020-0726**	N/A	O-MIC-WIND-180220/736
N/A	11-02-2020	6.8	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-0729**	N/A	O-MIC-WIND-180220/737
Improper Link Resolution Before File Access ('Link Following')	11-02-2020	3.6	An elevation of privilege vulnerability exists when the Windows User Profile Service (ProfSvc) improperly handles symlinks, aka 'Windows User Profile Service Elevation of Privilege Vulnerability'.	N/A	O-MIC-WIND-180220/738

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0730		
Improper Input Validation	11-02-2020	8.5	A remote code execution vulnerability exists in Remote Desktop Services â€“ formerly known as Terminal Services â€“ when an authenticated attacker abuses clipboard redirection, aka 'Remote Desktop ServicesÂ Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-0655**	N/A	O-MIC-WIND-180220/739
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory, aka 'Windows Common Log File System Driver Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0657**	N/A	O-MIC-WIND-180220/740
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists in the Windows Common Log File System (CLFS) driver when it fails to properly handle objects in memory, aka 'Windows Common Log File System Driver Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0658**	N/A	O-MIC-WIND-180220/741
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly	N/A	O-MIC-WIND-180220/742

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			handles file operations, aka 'Windows Data Sharing Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0747. **CVE ID : CVE-2020-0659**		
Improper Input Validation	11-02-2020	5	A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability'. **CVE ID : CVE-2020-0660**	N/A	O-MIC-WIND-180220/743
Improper Input Validation	11-02-2020	5.5	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2020-0751. **CVE ID : CVE-2020-0661**	N/A	O-MIC-WIND-180220/744
Improper Restriction of Operations within the Bounds of a Memory	11-02-2020	9	A remote code execution vulnerability exists in the way that Windows handles objects in memory, aka 'Windows Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-0662**	N/A	O-MIC-WIND-180220/745

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer					
Improper Privilege Management	11-02-2020	6.8	An elevation of privilege vulnerability exists in Active Directory Forest trusts due to a default setting that lets an attacker in the trusting forest request delegation of a TGT for an identity from the trusted forest, aka 'Active Directory Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0665**	N/A	O-MIC-WIND-180220/746
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0667, CVE-2020-0735, CVE-2020-0752. **CVE ID : CVE-2020-0666**	N/A	O-MIC-WIND-180220/747
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0666, CVE-2020-0735, CVE-2020-0752. **CVE ID : CVE-2020-0667**	N/A	O-MIC-WIND-180220/748
Improper	11-02-2020	4.6	An elevation of privilege	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0669, CVE-2020-0670, CVE-2020-0671, CVE-2020-0672. **CVE ID : CVE-2020-0668**		180220/749
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0668, CVE-2020-0670, CVE-2020-0671, CVE-2020-0672. **CVE ID : CVE-2020-0669**	N/A	O-MIC-WIND-180220/750
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0668, CVE-2020-0669, CVE-2020-0671, CVE-2020-0672. **CVE ID : CVE-2020-0670**	N/A	O-MIC-WIND-180220/751
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects	N/A	O-MIC-WIND-180220/752

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0668, CVE-2020-0669, CVE-2020-0670, CVE-2020-0672. **CVE ID : CVE-2020-0671**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0668, CVE-2020-0669, CVE-2020-0670, CVE-2020-0671. **CVE ID : CVE-2020-0672**	N/A	O-MIC-WIND-180220/753
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0674, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767. **CVE ID : CVE-2020-0673**	N/A	O-MIC-WIND-180220/754
Improper Restriction of Operations	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service	N/A	O-MIC-WIND-180220/755

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0676, CVE-2020-0677, CVE-2020-0748, CVE-2020-0755, CVE-2020-0756. **CVE ID : CVE-2020-0675**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from	N/A	O-MIC-WIND-180220/756

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-0675, CVE-2020-0677, CVE-2020-0748, CVE-2020-0755, CVE-2020-0756. **CVE ID : CVE-2020-0676**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0748, CVE-2020-0755, CVE-2020-0756. **CVE ID : CVE-2020-0677**	N/A	O-MIC-WIND-180220/757
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles hard links, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0678**	N/A	O-MIC-WIND-180220/758

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0680, CVE-2020-0682. **CVE ID : CVE-2020-0679**	N/A	O-MIC-WIND-180220/759
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0679, CVE-2020-0682. **CVE ID : CVE-2020-0680**	N/A	O-MIC-WIND-180220/760
Improper Input Validation	11-02-2020	7.6	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0734. **CVE ID : CVE-2020-0681**	N/A	O-MIC-WIND-180220/761
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in the way that the Windows	N/A	O-MIC-WIND-180220/762

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0679, CVE-2020-0680. **CVE ID : CVE-2020-0682**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in the Windows Installer when MSI packages process symbolic links, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0686. **CVE ID : CVE-2020-0683**	N/A	O-MIC-WIND-180220/763
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when Windows improperly handles COM object creation, aka 'Windows COM Server Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0685**	N/A	O-MIC-WIND-180220/764
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in the Windows Installer when MSI packages process symbolic links, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0683. **CVE ID : CVE-2020-0686**	N/A	O-MIC-WIND-180220/765

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	11-02-2020	4.6	A security feature bypass vulnerability exists in secure boot, aka 'Microsoft Secure Boot Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-0689**	N/A	O-MIC-WIND-180220/766
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists when the Telephony Service improperly discloses the contents of its memory, aka 'Windows Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0698**	N/A	O-MIC-WIND-180220/767
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Client License Service (ClipSVC) handles objects in memory, aka 'Windows Client License Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0701**	N/A	O-MIC-WIND-180220/768
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0703**	N/A	O-MIC-WIND-180220/769

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when the Windows Wireless Network Manager improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Wireless Network Manager Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0704**	N/A	O-MIC-WIND-180220/770
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists when the Windows Network Driver Interface Specification (NDIS) improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Network Driver Interface Specification (NDIS) Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0705**	N/A	O-MIC-WIND-180220/771
Information Exposure	11-02-2020	4.3	An information disclosure vulnerability exists in the way that affected Microsoft browsers handle cross-origin requests, aka 'Microsoft Browser Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0706**	N/A	O-MIC-WIND-180220/772

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when the Windows IME improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows IME Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0707**	N/A	O-MIC-WIND-180220/773
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0732. **CVE ID : CVE-2020-0709**	N/A	O-MIC-WIND-180220/774
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726. **CVE ID : CVE-2020-0731**	N/A	O-MIC-WIND-180220/775

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0709. **CVE ID : CVE-2020-0732**	N/A	O-MIC-WIND-180220/776
Improper Input Validation	11-02-2020	9.3	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0681. **CVE ID : CVE-2020-0734**	N/A	O-MIC-WIND-180220/777
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0666, CVE-2020-0667, CVE-2020-0752. **CVE ID : CVE-2020-0735**	N/A	O-MIC-WIND-180220/778
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the tapisrv.dll handles objects in memory, aka 'Windows	N/A	O-MIC-WIND-180220/779

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0739. **CVE ID : CVE-2020-0737**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	9.3	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. **CVE ID : CVE-2020-0738**	N/A	O-MIC-WIND-180220/780
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the dssvc.dll handles file creation allowing for a file overwrite or creation in a secured location, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0737. **CVE ID : CVE-2020-0739**	N/A	O-MIC-WIND-180220/781
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0741, CVE-2020-0742, CVE-2020-0743, CVE-2020-0749, CVE-2020-	N/A	O-MIC-WIND-180220/782

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0750. **CVE ID : CVE-2020-0740**		
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0740, CVE-2020-0742, CVE-2020-0743, CVE-2020-0749, CVE-2020-0750. **CVE ID : CVE-2020-0741**	N/A	O-MIC-WIND-180220/783
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0740, CVE-2020-0741, CVE-2020-0743, CVE-2020-0749, CVE-2020-0750. **CVE ID : CVE-2020-0742**	N/A	O-MIC-WIND-180220/784
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service	N/A	O-MIC-WIND-180220/785

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0740, CVE-2020-0741, CVE-2020-0742, CVE-2020-0749, CVE-2020-0750. **CVE ID : CVE-2020-0743**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an attacker to retrieve information from a targeted system, aka 'Windows GDI Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0744**	N/A	O-MIC-WIND-180220/786
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0715, CVE-2020-0792. **CVE ID : CVE-2020-0745**	N/A	O-MIC-WIND-180220/787
Information Exposure	11-02-2020	5	An information disclosure vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Information	N/A	O-MIC-WIND-180220/788

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability'. **CVE ID : CVE-2020-0746**		
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka 'Windows Data Sharing Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0659. **CVE ID : CVE-2020-0747**	N/A	O-MIC-WIND-180220/789
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0677, CVE-2020-0755, CVE-2020-0756. **CVE ID : CVE-2020-0748**	N/A	O-MIC-WIND-180220/790
Improper	11-02-2020	4.6	An elevation of privilege	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0740, CVE-2020-0741, CVE-2020-0742, CVE-2020-0743, CVE-2020-0750. **CVE ID : CVE-2020-0749**		180220/791
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0740, CVE-2020-0741, CVE-2020-0742, CVE-2020-0743, CVE-2020-0749. **CVE ID : CVE-2020-0750**	N/A	O-MIC-WIND-180220/792
Improper Input Validation	11-02-2020	2.1	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate specific malicious data from a user on a guest operating system.To exploit the vulnerability, an attacker who already has a privileged account on a	N/A	O-MIC-WIND-180220/793

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			guest operating system, running as a virtual machine, could run a specially crafted application.The security update addresses the vulnerability by resolving the conditions where Hyper-V would fail to handle these requests., aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2020-0661. **CVE ID : CVE-2020-0751**		
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0666, CVE-2020-0667, CVE-2020-0735. **CVE ID : CVE-2020-0752**	N/A	O-MIC-WIND-180220/794
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0754. **CVE ID : CVE-2020-0753**	N/A	O-MIC-WIND-180220/795
Improper	11-02-2020	4.6	An elevation of privilege	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0753. **CVE ID : CVE-2020-0754**		180220/796
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0677, CVE-2020-0748, CVE-2020-0756. **CVE ID : CVE-2020-0755**	N/A	O-MIC-WIND-180220/797
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly	N/A	O-MIC-WIND-180220/798

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0677, CVE-2020-0748, CVE-2020-0755. **CVE ID : CVE-2020-0756**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when Windows improperly handles Secure Socket Shell remote commands, aka 'Windows SSH Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0757**	N/A	O-MIC-WIND-180220/799
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0710, CVE-2020-0711,	N/A	O-MIC-WIND-180220/800

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-0712, CVE-2020-0713. **CVE ID : CVE-2020-0767**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0715, CVE-2020-0745. **CVE ID : CVE-2020-0792**	N/A	O-MIC-WIND-180220/801
windows_server_2019					
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767. **CVE ID : CVE-2020-0710**	N/A	O-MIC-WIND-180220/802
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-	N/A	O-MIC-WIND-180220/803

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-0674, CVE-2020-0710, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767. **CVE ID : CVE-2020-0711**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0710, CVE-2020-0711, CVE-2020-0713, CVE-2020-0767. **CVE ID : CVE-2020-0712**	N/A	O-MIC-WIND-180220/804
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0767. **CVE ID : CVE-2020-0713**	N/A	O-MIC-WIND-180220/805
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information	N/A	O-MIC-WIND-180220/806

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0716. **CVE ID : CVE-2020-0717**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0719**	N/A	O-MIC-WIND-180220/807
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0720**	N/A	O-MIC-WIND-180220/808
Improper	11-02-2020	7.2	An elevation of privilege	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0721**		180220/809
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0722**	N/A	O-MIC-WIND-180220/810
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege	N/A	O-MIC-WIND-180220/811

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0723**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0724**	N/A	O-MIC-WIND-180220/812
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723,	N/A	O-MIC-WIND-180220/813

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-0724, CVE-2020-0726, CVE-2020-0731. **CVE ID : CVE-2020-0725**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0731. **CVE ID : CVE-2020-0726**	N/A	O-MIC-WIND-180220/814
N/A	11-02-2020	6.8	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-0729**	N/A	O-MIC-WIND-180220/815
Improper Link Resolution Before File Access ('Link	11-02-2020	3.6	An elevation of privilege vulnerability exists when the Windows User Profile Service (ProfSvc) improperly handles	N/A	O-MIC-WIND-180220/816

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Following')			symlinks, aka 'Windows User Profile Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0730**		
Improper Input Validation	11-02-2020	8.5	A remote code execution vulnerability exists in Remote Desktop Services â€“ formerly known as Terminal Services â€“ when an authenticated attacker abuses clipboard redirection, aka 'Remote Desktop ServicesÂ Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-0655**	N/A	O-MIC-WIND-180220/817
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory, aka 'Windows Common Log File System Driver Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0657**	N/A	O-MIC-WIND-180220/818
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists in the Windows Common Log File System (CLFS) driver when it fails to properly handle objects in memory, aka 'Windows Common Log File System Driver Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0658**	N/A	O-MIC-WIND-180220/819

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka 'Windows Data Sharing Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0747. **CVE ID : CVE-2020-0659**	N/A	O-MIC-WIND-180220/820
Improper Input Validation	11-02-2020	5	A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability'. **CVE ID : CVE-2020-0660**	N/A	O-MIC-WIND-180220/821
Improper Input Validation	11-02-2020	5.5	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2020-0751. **CVE ID : CVE-2020-0661**	N/A	O-MIC-WIND-180220/822
Improper Restriction of	11-02-2020	9	A remote code execution vulnerability exists in the way that Windows handles	N/A	O-MIC-WIND-180220/823

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			objects in memory, aka 'Windows Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-0662**		
Improper Privilege Management	11-02-2020	4	An elevation of privilege vulnerability exists when Microsoft Edge does not properly enforce cross-domain policies, which could allow an attacker to access information from one domain and inject it into another domain.In a web-based attack scenario, an attacker could host a website that is used to attempt to exploit the vulnerability, aka 'Microsoft Edge Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0663**	N/A	O-MIC-WIND-180220/824
Improper Privilege Management	11-02-2020	6.8	An elevation of privilege vulnerability exists in Active Directory Forest trusts due to a default setting that lets an attacker in the trusting forest request delegation of a TGT for an identity from the trusted forest, aka 'Active Directory Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0665**	N/A	O-MIC-WIND-180220/825
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka	N/A	O-MIC-WIND-180220/826

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0667, CVE-2020-0735, CVE-2020-0752. **CVE ID : CVE-2020-0666**		
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0666, CVE-2020-0735, CVE-2020-0752. **CVE ID : CVE-2020-0667**	N/A	O-MIC-WIND-180220/827
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0669, CVE-2020-0670, CVE-2020-0671, CVE-2020-0672. **CVE ID : CVE-2020-0668**	N/A	O-MIC-WIND-180220/828
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from	N/A	O-MIC-WIND-180220/829

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-0668, CVE-2020-0670, CVE-2020-0671, CVE-2020-0672. **CVE ID : CVE-2020-0669**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0668, CVE-2020-0669, CVE-2020-0671, CVE-2020-0672. **CVE ID : CVE-2020-0670**	N/A	O-MIC-WIND-180220/830
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0668, CVE-2020-0669, CVE-2020-0670, CVE-2020-0672. **CVE ID : CVE-2020-0671**	N/A	O-MIC-WIND-180220/831
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0668, CVE-2020-0669, CVE-2020-0670, CVE-2020-0671.	N/A	O-MIC-WIND-180220/832

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0672		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0674, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767. **CVE ID : CVE-2020-0673**	N/A	O-MIC-WIND-180220/833
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767. **CVE ID : CVE-2020-0674**	N/A	O-MIC-WIND-180220/834
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an	N/A	O-MIC-WIND-180220/835

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0676, CVE-2020-0677, CVE-2020-0748, CVE-2020-0755, CVE-2020-0756. **CVE ID : CVE-2020-0675**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0677, CVE-2020-0748, CVE-2020-0755, CVE-2020-0756.	N/A	O-MIC-WIND-180220/836

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0676		
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0748, CVE-2020-0755, CVE-2020-0756. **CVE ID : CVE-2020-0677**	N/A	O-MIC-WIND-180220/837
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles hard links, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0678**	N/A	O-MIC-WIND-180220/838
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in	N/A	O-MIC-WIND-180220/839

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0680, CVE-2020-0682. **CVE ID : CVE-2020-0679**		
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0679, CVE-2020-0682. **CVE ID : CVE-2020-0680**	N/A	O-MIC-WIND-180220/840
Improper Input Validation	11-02-2020	7.6	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0734. **CVE ID : CVE-2020-0681**	N/A	O-MIC-WIND-180220/841
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege	N/A	O-MIC-WIND-180220/842

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. This CVE ID is unique from CVE-2020-0679, CVE-2020-0680. **CVE ID : CVE-2020-0682**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in the Windows Installer when MSI packages process symbolic links, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0686. **CVE ID : CVE-2020-0683**	N/A	O-MIC-WIND-180220/843
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when Windows improperly handles COM object creation, aka 'Windows COM Server Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0685**	N/A	O-MIC-WIND-180220/844
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in the Windows Installer when MSI packages process symbolic links, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0683. **CVE ID : CVE-2020-0686**	N/A	O-MIC-WIND-180220/845
Improper Input Validation	11-02-2020	4.6	A security feature bypass vulnerability exists in secure boot, aka 'Microsoft Secure Boot Security Feature Bypass	N/A	O-MIC-WIND-180220/846

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. **CVE ID : CVE-2020-0689**		
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists when the Telephony Service improperly discloses the contents of its memory, aka 'Windows Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0698**	N/A	O-MIC-WIND-180220/847
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Client License Service (ClipSVC) handles objects in memory, aka 'Windows Client License Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0701**	N/A	O-MIC-WIND-180220/848
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0703**	N/A	O-MIC-WIND-180220/849
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when the Windows Wireless Network Manager improperly handles memory.To exploit this	N/A	O-MIC-WIND-180220/850

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Wireless Network Manager Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0704**		
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists when the Windows Network Driver Interface Specification (NDIS) improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Network Driver Interface Specification (NDIS) Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0705**	N/A	O-MIC-WIND-180220/851
Information Exposure	11-02-2020	4.3	An information disclosure vulnerability exists in the way that affected Microsoft browsers handle cross-origin requests, aka 'Microsoft Browser Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0706**	N/A	O-MIC-WIND-180220/852
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when the Windows IME improperly handles memory.To exploit this vulnerability, an attacker	N/A	O-MIC-WIND-180220/853

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			would first have to gain execution on the victim system, aka 'Windows IME Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0707**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726. **CVE ID : CVE-2020-0731**	N/A	O-MIC-WIND-180220/854
Improper Input Validation	11-02-2020	9.3	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0681. **CVE ID : CVE-2020-0734**	N/A	O-MIC-WIND-180220/855
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles	N/A	O-MIC-WIND-180220/856

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0666, CVE-2020-0667, CVE-2020-0752. **CVE ID : CVE-2020-0735**		
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the tapisrv.dll handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0739. **CVE ID : CVE-2020-0737**	N/A	O-MIC-WIND-180220/857
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	9.3	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. **CVE ID : CVE-2020-0738**	N/A	O-MIC-WIND-180220/858
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the dssvc.dll handles file creation allowing for a file overwrite or creation in a secured location, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0737. **CVE ID : CVE-2020-0739**	N/A	O-MIC-WIND-180220/859

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0741, CVE-2020-0742, CVE-2020-0743, CVE-2020-0749, CVE-2020-0750. **CVE ID : CVE-2020-0740**	N/A	O-MIC-WIND-180220/860
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0740, CVE-2020-0742, CVE-2020-0743, CVE-2020-0749, CVE-2020-0750. **CVE ID : CVE-2020-0741**	N/A	O-MIC-WIND-180220/861
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-	N/A	O-MIC-WIND-180220/862

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0740, CVE-2020-0741, CVE-2020-0743, CVE-2020-0749, CVE-2020-0750. **CVE ID : CVE-2020-0742**		
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0740, CVE-2020-0741, CVE-2020-0742, CVE-2020-0749, CVE-2020-0750. **CVE ID : CVE-2020-0743**	N/A	O-MIC-WIND-180220/863
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an attacker to retrieve information from a targeted system, aka 'Windows GDI Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0744**	N/A	O-MIC-WIND-180220/864
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component	N/A	O-MIC-WIND-180220/865

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0715, CVE-2020-0792. **CVE ID : CVE-2020-0745**		
Information Exposure	11-02-2020	5	An information disclosure vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Information Disclosure Vulnerability'. **CVE ID : CVE-2020-0746**	N/A	O-MIC-WIND-180220/866
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka 'Windows Data Sharing Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0659. **CVE ID : CVE-2020-0747**	N/A	O-MIC-WIND-180220/867
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting	N/A	O-MIC-WIND-180220/868

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0677, CVE-2020-0755, CVE-2020-0756. **CVE ID : CVE-2020-0748**		
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0740, CVE-2020-0741, CVE-2020-0742, CVE-2020-0743, CVE-2020-0750. **CVE ID : CVE-2020-0749**	N/A	O-MIC-WIND-180220/869
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0740, CVE-2020-0741, CVE-2020-0742, CVE-2020-0743, CVE-2020-0749.	N/A	O-MIC-WIND-180220/870

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0750		
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0666, CVE-2020-0667, CVE-2020-0735. **CVE ID : CVE-2020-0752**	N/A	O-MIC-WIND-180220/871
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0754. **CVE ID : CVE-2020-0753**	N/A	O-MIC-WIND-180220/872
Improper Privilege Management	11-02-2020	4.6	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0753. **CVE ID : CVE-2020-0754**	N/A	O-MIC-WIND-180220/873
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service	N/A	O-MIC-WIND-180220/874

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0677, CVE-2020-0748, CVE-2020-0756. **CVE ID : CVE-2020-0755**		
Information Exposure	11-02-2020	2.1	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE ID is unique from	N/A	O-MIC-WIND-180220/875

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-0675, CVE-2020-0676, CVE-2020-0677, CVE-2020-0748, CVE-2020-0755. **CVE ID : CVE-2020-0756**		
Improper Privilege Management	11-02-2020	7.2	An elevation of privilege vulnerability exists when Windows improperly handles Secure Socket Shell remote commands, aka 'Windows SSH Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-0757**	N/A	O-MIC-WIND-180220/876
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-02-2020	7.6	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713. **CVE ID : CVE-2020-0767**	N/A	O-MIC-WIND-180220/877
surface_hub_firmware					
Incorrect Authorization	11-02-2020	4.6	A security feature bypass vulnerability exists in Surface Hub when prompting for credentials, aka 'Surface Hub Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-0702**	N/A	O-MIC-SURF-180220/878
Mikrotik					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
winbox					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-02-2020	4.3	MikroTik WinBox before 3.21 is vulnerable to a path traversal vulnerability that allows creation of arbitrary files wherevere WinBox has write permissions. WinBox is vulnerable to this attack if it connects to a malicious endpoint or if an attacker mounts a man in the middle attack. **CVE ID : CVE-2020-5720**	N/A	O-MIK-WINB-180220/879
Opensuse					
leap					
Uncontrolled Resource Consumption	07-02-2020	6.8	A flaw was found in the way the Ceph RGW Beast front-end handles unexpected disconnects. An authenticated attacker can abuse this flaw by making multiple disconnect attempts resulting in a permanent leak of a socket connection by radosgw. This flaw could lead to a denial of service condition by pile up of CLOSE_WAIT sockets, eventually leading to the exhaustion of available resources, preventing legitimate users from connecting to the system. **CVE ID : CVE-2020-1700**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1700	O-OPE-LEAP-180220/880
Missing Release of	05-02-2020	5	An ni_dhcp4_parse_response	http://lists.opensuse.org/	O-OPE-LEAP-180220/881

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource after Effective Lifetime			memory leak in openSUSE wicked 0.6.55 and earlier allows network attackers to cause a denial of service by sending DHCP4 packets without a message type option. **CVE ID : CVE-2020-7216**	opensuse-security-announce/2020-02/msg00005.html	
Redhat					
enterprise_linux					
Improper Authentication	12-02-2020	7.5	Istio 1.3 through 1.4.3 allows authentication bypass. The Authentication Policy exact-path matching logic can allow unauthorized access to HTTP paths even if they are configured to be only accessed after presenting a valid JWT token. For example, an attacker can add a ? or # character to a URI that would otherwise satisfy an exact-path match. **CVE ID : CVE-2020-8595**	https://access.redhat.com/security/cve/cve-2020-8595, https://istio.io/news/security/istio-security-2020-001/	O-RED-ENTE-180220/882
schmid-telecom					
zi_620_v400_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-02-2020	10	Schmid ZI 620 V400 VPN 090 routers allow an attacker to execute OS commands as root via shell metacharacters to an entry on the SSH subcommand menu, as demonstrated by ping. **CVE ID : CVE-2020-6760**	N/A	O-SCH-ZI_6-180220/883
ui					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
edgeswitch					
Improper Privilege Management	07-02-2020	7.2	A privilege escalation in the EdgeSwitch prior to version 1.7.1, an CGI script don't fully sanitize the user input resulting in local commands execution, allowing an operator user (Privilege-1) to escalate privileges and became administrator (Privilege-15). **CVE ID : CVE-2020-8126**	N/A	O-UI-EDGE-180220/884
Hardware					
automationdirect					
c-more_ea9-rhi					
Insufficiently Protected Credentials	05-02-2020	10	It is possible to unmask credentials and other sensitive information on “unprotected” project files, which may allow an attacker to remotely access the C-More Touch Panels EA9 series: firmware versions prior to 6.53 and manipulate system configurations. **CVE ID : CVE-2020-6969**	N/A	H-AUT-C-MO-180220/885
c-more_ea9-t6cl-r					
Insufficiently Protected Credentials	05-02-2020	10	It is possible to unmask credentials and other sensitive information on “unprotected” project files, which may allow an attacker to remotely access the C-More Touch Panels EA9 series: firmware versions prior to	N/A	H-AUT-C-MO-180220/886

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			6.53 and manipulate system configurations. **CVE ID : CVE-2020-6969**		
c-more_ea9-t6cl					
Insufficiently Protected Credentials	05-02-2020	10	It is possible to unmask credentials and other sensitive information on "unprotected" project files, which may allow an attacker to remotely access the C-More Touch Panels EA9 series: firmware versions prior to 6.53 and manipulate system configurations. **CVE ID : CVE-2020-6969**	N/A	H-AUT-C-MO-180220/887
c-more_ea9-t7cl-r					
Insufficiently Protected Credentials	05-02-2020	10	It is possible to unmask credentials and other sensitive information on "unprotected" project files, which may allow an attacker to remotely access the C-More Touch Panels EA9 series: firmware versions prior to 6.53 and manipulate system configurations. **CVE ID : CVE-2020-6969**	N/A	H-AUT-C-MO-180220/888
c-more_ea9-t7cl					
Insufficiently Protected Credentials	05-02-2020	10	It is possible to unmask credentials and other sensitive information on "unprotected" project files, which may allow an attacker to remotely access the C-More Touch Panels EA9 series:	N/A	H-AUT-C-MO-180220/889

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware versions prior to 6.53 and manipulate system configurations. **CVE ID : CVE-2020-6969**		
c-more_ea9-t8cl					
Insufficiently Protected Credentials	05-02-2020	10	It is possible to unmask credentials and other sensitive information on "unprotected" project files, which may allow an attacker to remotely access the C-More Touch Panels EA9 series: firmware versions prior to 6.53 and manipulate system configurations. **CVE ID : CVE-2020-6969**	N/A	H-AUT-C-MO-180220/890
c-more_ea9-t10cl					
Insufficiently Protected Credentials	05-02-2020	10	It is possible to unmask credentials and other sensitive information on "unprotected" project files, which may allow an attacker to remotely access the C-More Touch Panels EA9 series: firmware versions prior to 6.53 and manipulate system configurations. **CVE ID : CVE-2020-6969**	N/A	H-AUT-C-MO-180220/891
c-more_ea9-t10wcl					
Insufficiently Protected Credentials	05-02-2020	10	It is possible to unmask credentials and other sensitive information on "unprotected" project files, which may allow an attacker to remotely access the C-More Touch	N/A	H-AUT-C-MO-180220/892

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Panels EA9 series: firmware versions prior to 6.53 and manipulate system configurations. **CVE ID : CVE-2020-6969**		
c-more_ea9-t12cl					
Insufficiently Protected Credentials	05-02-2020	10	It is possible to unmask credentials and other sensitive information on "unprotected" project files, which may allow an attacker to remotely access the C-More Touch Panels EA9 series: firmware versions prior to 6.53 and manipulate system configurations. **CVE ID : CVE-2020-6969**	N/A	H-AUT-C-MO-180220/893
c-more_ea9-t15cl-r					
Insufficiently Protected Credentials	05-02-2020	10	It is possible to unmask credentials and other sensitive information on "unprotected" project files, which may allow an attacker to remotely access the C-More Touch Panels EA9 series: firmware versions prior to 6.53 and manipulate system configurations. **CVE ID : CVE-2020-6969**	N/A	H-AUT-C-MO-180220/894
c-more_ea9-t15cl					
Insufficiently Protected Credentials	05-02-2020	10	It is possible to unmask credentials and other sensitive information on "unprotected" project files, which may allow an attacker to remotely	N/A	H-AUT-C-MO-180220/895

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access the C-More Touch Panels EA9 series: firmware versions prior to 6.53 and manipulate system configurations. **CVE ID : CVE-2020-6969**		
bosch					
divar_ip_2000					
Missing Authentication for Critical Function	07-02-2020	6.4	Missing Authentication for Critical Function in the Bosch Video Streaming Gateway (VSG) allows an unauthenticated remote attacker to retrieve and set arbitrary configuration data of the Video Streaming Gateway. A successful attack can impact the confidentiality and availability of live and recorded video data of all cameras configured to be controlled by the VSG as well as the recording storage associated with the VSG. This affects Bosch Video Streaming Gateway versions 6.45 <= 6.45.08, 6.44 <= 6.44.022, 6.43 <= 6.43.0023 and 6.42.10 and older. This affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR IP all-in-one 5000 if a vulnerable VSG version is installed with BVMS. This affects Bosch DIVAR IP 2000 <= 3.62.0019 and DIVAR IP 5000 <= 3.80.0039 if the corresponding port 8023	https://psirt.bosch.com/security-advisories/BOSCH-SA-260625-BT.html	H-BOS-DIVA-180220/896

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			has been opened in the device's firewall. **CVE ID : CVE-2020-6769**		
divar_ip_5000					
Missing Authentication on for Critical Function	07-02-2020	6.4	Missing Authentication for Critical Function in the Bosch Video Streaming Gateway (VSG) allows an unauthenticated remote attacker to retrieve and set arbitrary configuration data of the Video Streaming Gateway. A successful attack can impact the confidentiality and availability of live and recorded video data of all cameras configured to be controlled by the VSG as well as the recording storage associated with the VSG. This affects Bosch Video Streaming Gateway versions 6.45 <= 6.45.08, 6.44 <= 6.44.022, 6.43 <= 6.43.0023 and 6.42.10 and older. This affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR IP all-in-one 5000 if a vulnerable VSG version is installed with BVMS. This affects Bosch DIVAR IP 2000 <= 3.62.0019 and DIVAR IP 5000 <= 3.80.0039 if the corresponding port 8023 has been opened in the device's firewall. **CVE ID : CVE-2020-6769**	https://psirt.bosch.com/security-advisories/BOSCH-SA-260625-BT.html	H-BOS-DIVA-180220/897

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
divar_ip_3000					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-02-2020	5	A path traversal vulnerability in the Bosch Video Management System (BVMS) NoTouch deployment allows an unauthenticated remote attacker to read arbitrary files from the Central Server. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch BVMS Viewer versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR IP all-in-one 5000 if a vulnerable BVMS version is installed. **CVE ID : CVE-2020-6768**	https://psirt.bosch.com/security-advisories/bosch-sa-815013-bt.html	H-BOS-DIVA-180220/898
Missing Authentication for Critical Function	07-02-2020	6.4	Missing Authentication for Critical Function in the Bosch Video Streaming Gateway (VSG) allows an unauthenticated remote attacker to retrieve and set arbitrary configuration data of the Video Streaming Gateway. A successful attack can impact the confidentiality and availability of live and recorded video data of all cameras configured to be controlled by the VSG as	https://psirt.bosch.com/security-advisories/BOSCH-SA-260625-BT.html	H-BOS-DIVA-180220/899

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			well as the recording storage associated with the VSG. This affects Bosch Video Streaming Gateway versions 6.45 <= 6.45.08, 6.44 <= 6.44.022, 6.43 <= 6.43.0023 and 6.42.10 and older. This affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR IP all-in-one 5000 if a vulnerable VSG version is installed with BVMS. This affects Bosch DIVAR IP 2000 <= 3.62.0019 and DIVAR IP 5000 <= 3.80.0039 if the corresponding port 8023 has been opened in the device's firewall. **CVE ID : CVE-2020-6769**		
Deserialization of Untrusted Data	07-02-2020	10	Deserialization of Untrusted Data in the BVMS Mobile Video Service (BVMS MVS) allows an unauthenticated remote attacker to execute arbitrary code on the system. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000 and DIVAR IP 7000 if a vulnerable BVMS version is installed. **CVE ID : CVE-2020-6770**	https://psirt.bosch.com/security-advisories/BOSCH-SA-885551-BT.html	H-BOS-DIVA-180220/900
Improper Limitation of a Pathname	06-02-2020	4	A path traversal vulnerability in the Bosch Video Management System	https://psirt.bosch.com/security-	H-BOS-DIVA-180220/901

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			(BVMS) FileTransferService allows an authenticated remote attacker to read arbitrary files from the Central Server. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch BVMS Viewer versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR IP all-in-one 5000 if a vulnerable BVMS version is installed. **CVE ID : CVE-2020-6767**	advisories/BOSCH-SA-381489-BT.html	
divar_ip_7000					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-02-2020	5	A path traversal vulnerability in the Bosch Video Management System (BVMS) NoTouch deployment allows an unauthenticated remote attacker to read arbitrary files from the Central Server. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch BVMS Viewer versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This	https://psirt.bosch.com/security-advisories/bosch-sa-815013-bt.html	H-BOS-DIVA-180220/902

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR IP all-in-one 5000 if a vulnerable BVMS version is installed. **CVE ID : CVE-2020-6768**		
Missing Authenticati on for Critical Function	07-02-2020	6.4	Missing Authentication for Critical Function in the Bosch Video Streaming Gateway (VSG) allows an unauthenticated remote attacker to retrieve and set arbitrary configuration data of the Video Streaming Gateway. A successful attack can impact the confidentiality and availability of live and recorded video data of all cameras configured to be controlled by the VSG as well as the recording storage associated with the VSG. This affects Bosch Video Streaming Gateway versions 6.45 <= 6.45.08, 6.44 <= 6.44.022, 6.43 <= 6.43.0023 and 6.42.10 and older. This affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR IP all-in-one 5000 if a vulnerable VSG version is installed with BVMS. This affects Bosch DIVAR IP 2000 <= 3.62.0019 and DIVAR IP 5000 <= 3.80.0039 if the corresponding port 8023 has been opened in the device's firewall.	https://psirt.bosch.com/security-advisories/BOSCH-SA-260625-BT.html	H-BOS-DIVA-180220/903

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-6769		
Deserialization of Untrusted Data	07-02-2020	10	Deserialization of Untrusted Data in the BVMS Mobile Video Service (BVMS MVS) allows an unauthenticated remote attacker to execute arbitrary code on the system. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000 and DIVAR IP 7000 if a vulnerable BVMS version is installed. **CVE ID : CVE-2020-6770**	https://psirt.bosch.com/security-advisories/BOSCH-SA-885551-BT.html	H-BOS-DIVA-180220/904
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-02-2020	4	A path traversal vulnerability in the Bosch Video Management System (BVMS) FileTransferService allows an authenticated remote attacker to read arbitrary files from the Central Server. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch BVMS Viewer versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR IP all-in-one 5000 if a vulnerable BVMS version	https://psirt.bosch.com/security-advisories/BOSCH-SA-381489-BT.html	H-BOS-DIVA-180220/905

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is installed. **CVE ID : CVE-2020-6767**		
divar_ip_all-in-one_5000					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-02-2020	5	A path traversal vulnerability in the Bosch Video Management System (BVMS) NoTouch deployment allows an unauthenticated remote attacker to read arbitrary files from the Central Server. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch BVMS Viewer versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR IP all-in-one 5000 if a vulnerable BVMS version is installed. **CVE ID : CVE-2020-6768**	https://psirt.bosch.com/security-advisories/bosch-sa-815013-bt.html	H-BOS-DIVA-180220/906
Missing Authentication for Critical Function	07-02-2020	6.4	Missing Authentication for Critical Function in the Bosch Video Streaming Gateway (VSG) allows an unauthenticated remote attacker to retrieve and set arbitrary configuration data of the Video Streaming Gateway. A successful attack can impact the confidentiality and availability of live and recorded video data of all	https://psirt.bosch.com/security-advisories/BOSCH-SA-260625-BT.html	H-BOS-DIVA-180220/907

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cameras configured to be controlled by the VSG as well as the recording storage associated with the VSG. This affects Bosch Video Streaming Gateway versions 6.45 <= 6.45.08, 6.44 <= 6.44.022, 6.43 <= 6.43.0023 and 6.42.10 and older. This affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR IP all-in-one 5000 if a vulnerable VSG version is installed with BVMS. This affects Bosch DIVAR IP 2000 <= 3.62.0019 and DIVAR IP 5000 <= 3.80.0039 if the corresponding port 8023 has been opened in the device's firewall. **CVE ID : CVE-2020-6769**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-02-2020	4	A path traversal vulnerability in the Bosch Video Management System (BVMS) FileTransferService allows an authenticated remote attacker to read arbitrary files from the Central Server. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch BVMS Viewer versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch DIVAR IP	https://psirt.bosch.com/security-advisories/BOSCH-SA-381489-BT.html	H-BOS-DIVA-180220/908

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3000, DIVAR IP 7000 and DIVAR IP all-in-one 5000 if a vulnerable BVMS version is installed. **CVE ID : CVE-2020-6767**		
Cisco					
nexus_1000v					
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	N/A	H-CIS-NEXU-180220/909

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3120		
nexus_31128pq					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**	N/A	H-CIS-NEXU-180220/910
Integer	05-02-2020	6.1	A vulnerability in the Cisco	N/A	H-CIS-NEXU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow or Wraparound			Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		180220/911
nexus_3132c-z					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to	N/A	H-CIS-NEXU-180220/912

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of	N/A	H-CIS-NEXU-180220/913

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_3132q					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol	N/A	H-CIS-NEXU-180220/914

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery	N/A	H-CIS-NEXU-180220/915

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_3132q-v					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could	N/A	H-CIS-NEXU-180220/916

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this	N/A	H-CIS-NEXU-180220/917

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_3132q-xl					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same	N/A	H-CIS-NEXU-180220/918

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**	N/A	H-CIS-NEXU-180220/919
nexus_3164q					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**	N/A	H-CIS-NEXU-180220/920
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS	N/A	H-CIS-NEXU-180220/921

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_3172					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The	N/A	H-CIS-NEXU-180220/922

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the	N/A	H-CIS-NEXU-180220/923

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_3172pq-xl					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious	N/A	H-CIS-NEXU-180220/924

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could	N/A	H-CIS-NEXU-180220/925

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_3172tq					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative	N/A	H-CIS-NEXU-180220/926

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the	N/A	H-CIS-NEXU-180220/927

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_3172tq-32t					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	N/A	H-CIS-NEXU-180220/928

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3119		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**	N/A	H-CIS-NEXU-180220/929
nexus_3172tq-xl					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could	N/A	H-CIS-NEXU-180220/930

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload	N/A	H-CIS-NEXU-180220/931

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_3264c-e					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate	N/A	H-CIS-NEXU-180220/932

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this	N/A	H-CIS-NEXU-180220/933

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_3264q					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the	N/A	H-CIS-NEXU-180220/934

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery	N/A	H-CIS-NEXU-180220/935

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_3408-s					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this	N/A	H-CIS-NEXU-180220/936

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**	N/A	H-CIS-NEXU-180220/937

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
nexus_34180yc					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**	N/A	H-CIS-NEXU-180220/938
Integer Overflow or	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol	N/A	H-CIS-NEXU-180220/939

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_3432d-s					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or	N/A	H-CIS-NEXU-180220/940

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition.	N/A	H-CIS-NEXU-180220/941

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_3464c					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could	N/A	H-CIS-NEXU-180220/942

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an	N/A	H-CIS-NEXU-180220/943

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_3524					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to	N/A	H-CIS-NEXU-180220/944

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker	N/A	H-CIS-NEXU-180220/945

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_3524-x					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the	N/A	H-CIS-NEXU-180220/946

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**	N/A	H-CIS-NEXU-180220/947
nexus_3524-xl					
Out-of-bounds	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol	N/A	H-CIS-NEXU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		180220/948
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an	N/A	H-CIS-NEXU-180220/949

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_3548					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco	N/A	H-CIS-NEXU-180220/950

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery	N/A	H-CIS-NEXU-180220/951

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_3548-x					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected	N/A	H-CIS-NEXU-180220/952

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory,	N/A	H-CIS-NEXU-180220/953

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_3548-xl					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery	N/A	H-CIS-NEXU-180220/954

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2	N/A	H-CIS-NEXU-180220/955

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			adjacent). **CVE ID : CVE-2020-3120**		
nexus_5548p					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**	N/A	H-CIS-NEXU-180220/956

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**	N/A	H-CIS-NEXU-180220/957
nexus_5548up					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated,	N/A	H-CIS-NEXU-180220/958

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device,	N/A	H-CIS-NEXU-180220/959

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_5596t					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a	N/A	H-CIS-NEXU-180220/960

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a	N/A	H-CIS-NEXU-180220/961

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_5596up					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack	N/A	H-CIS-NEXU-180220/962

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2	N/A	H-CIS-NEXU-180220/963

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_56128p					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker	N/A	H-CIS-NEXU-180220/964

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**	N/A	H-CIS-NEXU-180220/965
nexus_5624q					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**	N/A	H-CIS-NEXU-180220/966
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS	N/A	H-CIS-NEXU-180220/967

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_5648q					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The	N/A	H-CIS-NEXU-180220/968

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the	N/A	H-CIS-NEXU-180220/969

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_5672up					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious	N/A	H-CIS-NEXU-180220/970

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could	N/A	H-CIS-NEXU-180220/971

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_5696q					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative	N/A	H-CIS-NEXU-180220/972

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the	N/A	H-CIS-NEXU-180220/973

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_6001					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	N/A	H-CIS-NEXU-180220/974

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3119		
nexus_6004					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**	N/A	H-CIS-NEXU-180220/975
asr_9000v					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**	N/A	H-CIS-ASR_-180220/976
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an	N/A	H-CIS-ASR_-180220/977

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
asr_9001					
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of	N/A	H-CIS-ASR_-180220/978

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this	N/A	H-CIS-ASR_-180220/979

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
asr_9006					
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which	N/A	H-CIS-ASR_-180220/980

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this	N/A	H-CIS-ASR_-180220/981

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
asr_9010					
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2	N/A	H-CIS-ASR_-180220/982

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			adjacent). **CVE ID : CVE-2020-3118**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**	N/A	H-CIS-ASR_-180220/983
asr_9901					
Use of Externally-Controlled	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco	N/A	H-CIS-ASR_-180220/984

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Format String			IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device,	N/A	H-CIS-ASR_-180220/985

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
asr_9904					
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An	N/A	H-CIS-ASR_-180220/986

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an	N/A	H-CIS-ASR_-180220/987

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
asr_9906					
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative	N/A	H-CIS-ASR_-180220/988

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the	N/A	H-CIS-ASR_-180220/989

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
asr_9910					
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**	N/A	H-CIS-ASR_-180220/990

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**	N/A	H-CIS-ASR_-180220/991
asr_9912					
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated,	N/A	H-CIS-ASR_-180220/992

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition.	N/A	H-CIS-ASR_-180220/993

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
asr_9922					
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a	N/A	H-CIS-ASR_-180220/994

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could	N/A	H-CIS-ASR_-180220/995

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_36180yc-r					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative	N/A	H-CIS-NEXU-180220/996

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the	N/A	H-CIS-NEXU-180220/997

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_3636c-r					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	N/A	H-CIS-NEXU-180220/998

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3119		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**	N/A	H-CIS-NEXU-180220/999
nexus_7000					
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS	N/A	H-CIS-NEXU-180220/1000

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_7700					
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device,	N/A	H-CIS-NEXU-180220/1001

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
ip_conference_phone_8832					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An	N/A	H-CIS-IP_C-180220/1002

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
ip_phone_7811					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the	N/A	H-CIS-IP_P-180220/1003

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
ip_phone_7821					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code	N/A	H-CIS-IP_P-180220/1004

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
ip_phone_7841					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of	N/A	H-CIS-IP_P-180220/1005

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
ip_phone_7861					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability,	N/A	H-CIS-IP_P-180220/1006

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
ip_phone_8811					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	N/A	H-CIS-IP_P-180220/1007

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3111		
ip_phone_8841					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**	N/A	H-CIS-IP_P-180220/1008
ip_phone_8845					
Improper Input	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol	N/A	H-CIS-IP_P-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		180220/1009
ip_phone_8851					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to	N/A	H-CIS-IP_P-180220/1010

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
ip_phone_8861					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The	N/A	H-CIS-IP_P-180220/1011

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
ip_phone_8865					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An	N/A	H-CIS-IP_P-180220/1012

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
wireless_ip_phone_8821					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the	N/A	H-CIS-WIRE-180220/1013

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
wireless_ip_phone_8821-ex					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code	N/A	H-CIS-WIRE-180220/1014

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
firepower_9300					
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery	N/A	H-CIS-FIRE-180220/1015

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
firepower_4115					
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the	N/A	H-CIS-FIRE-180220/1016

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
firepower_4125					
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**	N/A	H-CIS-FIRE-180220/1017
firepower_4145					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**	N/A	H-CIS-FIRE-180220/1018
firepower_4110					
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-	N/A	H-CIS-FIRE-180220/1019

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
firepower_4120					
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of	N/A	H-CIS-FIRE-180220/1020

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
firepower_4140					
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery	N/A	H-CIS-FIRE-180220/1021

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
firepower_4150					
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an	N/A	H-CIS-FIRE-180220/1022

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
video_surveillance_8400_ip_camera					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco Video Surveillance 8000 Series IP Cameras could allow an unauthenticated, adjacent attacker to execute code remotely or cause a reload of an affected IP Camera. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to the targeted IP Camera. A successful exploit could allow the attacker to expose the affected IP Camera for remote code execution or cause it to reload unexpectedly,	N/A	H-CIS-VIDE-180220/1023

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). This vulnerability is fixed in Video Surveillance 8000 Series IP Camera Firmware Release 1.0.7 and later. **CVE ID : CVE-2020-3110**		
video_surveillance_8030_ip_camera					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco Video Surveillance 8000 Series IP Cameras could allow an unauthenticated, adjacent attacker to execute code remotely or cause a reload of an affected IP Camera. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to the targeted IP Camera. A successful exploit could allow the attacker to expose the affected IP Camera for remote code execution or cause it to	N/A	H-CIS-VIDE-180220/1024

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reload unexpectedly, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). This vulnerability is fixed in Video Surveillance 8000 Series IP Camera Firmware Release 1.0.7 and later. **CVE ID : CVE-2020-3110**		
video_surveillance_8020_ip_camera					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco Video Surveillance 8000 Series IP Cameras could allow an unauthenticated, adjacent attacker to execute code remotely or cause a reload of an affected IP Camera. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to the targeted IP Camera. A successful exploit could allow the attacker to expose the affected IP Camera for remote code	N/A	H-CIS-VIDE-180220/1025

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution or cause it to reload unexpectedly, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). This vulnerability is fixed in Video Surveillance 8000 Series IP Camera Firmware Release 1.0.7 and later. **CVE ID : CVE-2020-3110**		
video_surveillance_8000p_ip_camera					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco Video Surveillance 8000 Series IP Cameras could allow an unauthenticated, adjacent attacker to execute code remotely or cause a reload of an affected IP Camera. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to the targeted IP Camera. A successful exploit could allow the attacker to expose the affected IP	N/A	H-CIS-VIDE-180220/1026

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Camera for remote code execution or cause it to reload unexpectedly, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). This vulnerability is fixed in Video Surveillance 8000 Series IP Camera Firmware Release 1.0.7 and later. **CVE ID : CVE-2020-3110**		
video_surveillance_8930_speed_dome_ip_camera					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco Video Surveillance 8000 Series IP Cameras could allow an unauthenticated, adjacent attacker to execute code remotely or cause a reload of an affected IP Camera. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to the targeted IP Camera. A successful exploit could allow the attacker to	N/A	H-CIS-VIDE-180220/1027

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			expose the affected IP Camera for remote code execution or cause it to reload unexpectedly, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). This vulnerability is fixed in Video Surveillance 8000 Series IP Camera Firmware Release 1.0.7 and later. **CVE ID : CVE-2020-3110**		
video_surveillance_8630_ip_camera					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco Video Surveillance 8000 Series IP Cameras could allow an unauthenticated, adjacent attacker to execute code remotely or cause a reload of an affected IP Camera. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to the targeted IP Camera. A successful exploit could	N/A	H-CIS-VIDE-180220/1028

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to expose the affected IP Camera for remote code execution or cause it to reload unexpectedly, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). This vulnerability is fixed in Video Surveillance 8000 Series IP Camera Firmware Release 1.0.7 and later. **CVE ID : CVE-2020-3110**		
video_surveillance_8070_ip_camera					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco Video Surveillance 8000 Series IP Cameras could allow an unauthenticated, adjacent attacker to execute code remotely or cause a reload of an affected IP Camera. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to the targeted IP Camera. A	N/A	H-CIS-VIDE-180220/1029

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to expose the affected IP Camera for remote code execution or cause it to reload unexpectedly, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). This vulnerability is fixed in Video Surveillance 8000 Series IP Camera Firmware Release 1.0.7 and later. **CVE ID : CVE-2020-3110**		
video_surveillance_8620_ip_camera					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco Video Surveillance 8000 Series IP Cameras could allow an unauthenticated, adjacent attacker to execute code remotely or cause a reload of an affected IP Camera. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to the	N/A	H-CIS-VIDE-180220/1030

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			targeted IP Camera. A successful exploit could allow the attacker to expose the affected IP Camera for remote code execution or cause it to reload unexpectedly, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). This vulnerability is fixed in Video Surveillance 8000 Series IP Camera Firmware Release 1.0.7 and later. **CVE ID : CVE-2020-3110**		
ip_phone_6821					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery	N/A	H-CIS-IP_P-180220/1031

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
ucs_6248up					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful	N/A	H-CIS-UCS_-180220/1032

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to	N/A	H-CIS-UCS_-180220/1033

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
ucs_6296up					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2	N/A	H-CIS-UCS_-180220/1034

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	N/A	H-CIS-UCS_-180220/1035

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3120		
mds_9132t					
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**	N/A	H-CIS-MDS_-180220/1036
mds_9148s					
Integer Overflow or	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco	N/A	H-CIS-MDS_-180220/1037

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
mds_9148t					
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload	N/A	H-CIS-MDS_-180220/1038

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
mds_9216					
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the	N/A	H-CIS-MDS_-180220/1039

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
mds_9216a					
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a	N/A	H-CIS-MDS_-180220/1040

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
mds_9216i					
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to	N/A	H-CIS-MDS_-180220/1041

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
mds_9222i					
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this	N/A	H-CIS-MDS_-180220/1042

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
mds_9506					
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	N/A	H-CIS-MDS_-180220/1043

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3120		
mds_9509					
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**	N/A	H-CIS-MDS_-180220/1044
mds_9513					
Integer Overflow or	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco	N/A	H-CIS-MDS_-180220/1045

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
mds_9706					
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload	N/A	H-CIS-MDS_-180220/1046

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
mds_9710					
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the	N/A	H-CIS-MDS_-180220/1047

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
mds_9718					
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a	N/A	H-CIS-MDS_-180220/1048

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
ucs_6324					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack	N/A	H-CIS-UCS_-180220/1049

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2	N/A	H-CIS-UCS_-180220/1050

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
ip_conference_phone_7832					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as	N/A	H-CIS-IP_C-180220/1051

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
ip_phone_6841					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**	N/A	H-CIS-IP_P-180220/1052

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ip_phone_6851					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**	N/A	H-CIS-IP_P-180220/1053
ip_phone_6861					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the	N/A	H-CIS-IP_P-180220/1054

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
ip_phone_6871					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code	N/A	H-CIS-IP_P-180220/1055

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
unified_ip_conference_phone_8831					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to	N/A	H-CIS-UNIF-180220/1056

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
unified_ip_conference_phone_8831_for_third-party_call_control					
Improper Input Validation	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this	N/A	H-CIS-UNIF-180220/1057

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3111**		
crs					
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A	N/A	H-CIS-CRS-180220/1058

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to	N/A	H-CIS-CRS-180220/1059

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
ncs_1001					
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker	N/A	H-CIS-NCS_-180220/1060

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**		
ncs_1002					
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	N/A	H-CIS-NCS_-180220/1061

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3118		
ncs_1004					
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**	N/A	H-CIS-NCS_-180220/1062
ncs_520					
Use of Externally-	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol	N/A	H-CIS-NCS_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Controlled Format String			implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**		180220/1063
ncs_540-12z20g-sys-a					
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to	N/A	H-CIS-NCS_-180220/1064

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to	N/A	H-CIS-NCS_-180220/1065

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
ncs_540-12z20g-sys-d					
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery	N/A	H-CIS-NCS_-180220/1066

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to	N/A	H-CIS-NCS_-180220/1067

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
ncs_540-24z8q2c-sys					
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2	N/A	H-CIS-NCS_-180220/1068

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	N/A	H-CIS-NCS_-180220/1069

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3120		
ncs_540-28z4c-sys-a					
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**	N/A	H-CIS-NCS_-180220/1070
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco	N/A	H-CIS-NCS_-180220/1071

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
ncs_540-28z4c-sys-d					
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an	N/A	H-CIS-NCS_-180220/1072

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software	N/A	H-CIS-NCS_-180220/1073

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
ncs_540-acc-sys					
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A	N/A	H-CIS-NCS_-180220/1074

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to	N/A	H-CIS-NCS_-180220/1075

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
ncs_540x-12z16g-sys-a					
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker	N/A	H-CIS-NCS_-180220/1076

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**	N/A	H-CIS-NCS_-180220/1077
ncs_540x-12z16g-sys-d					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**	N/A	H-CIS-NCS_-180220/1078
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an	N/A	H-CIS-NCS_-180220/1079

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
ncs_540x-16z4g8q2c-a					
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of	N/A	H-CIS-NCS_-180220/1080

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this	N/A	H-CIS-NCS_-180220/1081

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
ncs_540x-16z4g8q2c-d					
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which	N/A	H-CIS-NCS_-180220/1082

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this	N/A	H-CIS-NCS_-180220/1083

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
ncs_540x-acc-sys					
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2	N/A	H-CIS-NCS_-180220/1084

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			adjacent). **CVE ID : CVE-2020-3118**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**	N/A	H-CIS-NCS_-180220/1085
ncs_5501					
Use of Externally-Controlled	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco	N/A	H-CIS-NCS_-180220/1086

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Format String			IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device,	N/A	H-CIS-NCS_-180220/1087

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
ncs_5501-se					
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An	N/A	H-CIS-NCS_-180220/1088

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an	N/A	H-CIS-NCS_-180220/1089

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
ncs_5502					
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative	N/A	H-CIS-NCS_-180220/1090

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the	N/A	H-CIS-NCS_-180220/1091

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
ncs_5502-se					
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**	N/A	H-CIS-NCS_-180220/1092

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**	N/A	H-CIS-NCS_-180220/1093
ncs_5508					
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated,	N/A	H-CIS-NCS_-180220/1094

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition.	N/A	H-CIS-NCS_-180220/1095

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
ncs_5516					
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a	N/A	H-CIS-NCS_-180220/1096

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could	N/A	H-CIS-NCS_-180220/1097

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
ncs_6000					
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery	N/A	H-CIS-NCS_-180220/1098

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2	N/A	H-CIS-NCS_-180220/1099

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			adjacent). **CVE ID : CVE-2020-3120**		
ncs_5001					
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**	N/A	H-CIS-NCS_-180220/1100
Integer Overflow or	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol	N/A	H-CIS-NCS_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		180220/1101
ncs_5002					
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or	N/A	H-CIS-NCS_-180220/1102

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the	N/A	H-CIS-NCS_-180220/1103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
ncs_5011					
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an	N/A	H-CIS-NCS_-180220/1104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory,	N/A	H-CIS-NCS_-180220/1105

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
ncs_540					
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this	N/A	H-CIS-NCS_-180220/1106

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**		
xrv_9000					
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2	N/A	H-CIS-XRV_-180220/1107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			adjacent). **CVE ID : CVE-2020-3118**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**	N/A	H-CIS-XRV_-180220/1108
ncs_560					
Use of Externally-Controlled	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco	N/A	H-CIS-NCS_-180220/1109

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Format String			IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device,	N/A	H-CIS-NCS_-180220/1110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
ncs_540l					
Use of Externally-Controlled Format String	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An	N/A	H-CIS-NCS_-180220/1111

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3118**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an	N/A	H-CIS-NCS_-180220/1112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_3232c_					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to	N/A	H-CIS-NEXU-180220/1113

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker	N/A	H-CIS-NEXU-180220/1114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
ucs_64108					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the	N/A	H-CIS-UCS_-180220/1115

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**	N/A	H-CIS-UCS_-180220/1116
ucs_6454					
Out-of-bounds	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol	N/A	H-CIS-UCS_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		180220/1117
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an	N/A	H-CIS-UCS_-180220/1118

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_1000ve					
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition.	N/A	H-CIS-NEXU-180220/1119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
ucs_6300					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could	N/A	H-CIS-UCS_-180220/1120

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an	N/A	H-CIS-UCS_-180220/1121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_9000v					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to	N/A	H-CIS-NEXU-180220/1122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker	N/A	H-CIS-NEXU-180220/1123

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_92160yc-x					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the	N/A	H-CIS-NEXU-180220/1124

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**	N/A	H-CIS-NEXU-180220/1125
nexus_92300yc					
Out-of-bounds	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol	N/A	H-CIS-NEXU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		180220/1126
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an	N/A	H-CIS-NEXU-180220/1127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_92304qc					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco	N/A	H-CIS-NEXU-180220/1128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery	N/A	H-CIS-NEXU-180220/1129

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_92348gc-x					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected	N/A	H-CIS-NEXU-180220/1130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory,	N/A	H-CIS-NEXU-180220/1131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_9236c					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery	N/A	H-CIS-NEXU-180220/1132

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2	N/A	H-CIS-NEXU-180220/1133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			adjacent). **CVE ID : CVE-2020-3120**		
nexus_9272q					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**	N/A	H-CIS-NEXU-180220/1134

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**	N/A	H-CIS-NEXU-180220/1135
nexus_93108tc-ex					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated,	N/A	H-CIS-NEXU-180220/1136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device,	N/A	H-CIS-NEXU-180220/1137

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_93108tc-fx					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a	N/A	H-CIS-NEXU-180220/1138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a	N/A	H-CIS-NEXU-180220/1139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_93120tx					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack	N/A	H-CIS-NEXU-180220/1140

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2	N/A	H-CIS-NEXU-180220/1141

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_93128tx					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker	N/A	H-CIS-NEXU-180220/1142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**	N/A	H-CIS-NEXU-180220/1143
nexus_93180lc-ex					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**	N/A	H-CIS-NEXU-180220/1144
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS	N/A	H-CIS-NEXU-180220/1145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_93180yc-ex					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The	N/A	H-CIS-NEXU-180220/1146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the	N/A	H-CIS-NEXU-180220/1147

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_93180yc-fx					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious	N/A	H-CIS-NEXU-180220/1148

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could	N/A	H-CIS-NEXU-180220/1149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_93216tc-fx2					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative	N/A	H-CIS-NEXU-180220/1150

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the	N/A	H-CIS-NEXU-180220/1151

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_93240yc-fx2					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	N/A	H-CIS-NEXU-180220/1152

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3119		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**	N/A	H-CIS-NEXU-180220/1153
nexus_9332c					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could	N/A	H-CIS-NEXU-180220/1154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload	N/A	H-CIS-NEXU-180220/1155

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_9332pq					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate	N/A	H-CIS-NEXU-180220/1156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this	N/A	H-CIS-NEXU-180220/1157

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_93360yc-fx2					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the	N/A	H-CIS-NEXU-180220/1158

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery	N/A	H-CIS-NEXU-180220/1159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_9336c-fx2					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this	N/A	H-CIS-NEXU-180220/1160

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**	N/A	H-CIS-NEXU-180220/1161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
nexus_9336pq_aci_spine					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**	N/A	H-CIS-NEXU-180220/1162
Integer Overflow or	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol	N/A	H-CIS-NEXU-180220/1163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_9348gc-fxp					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or	N/A	H-CIS-NEXU-180220/1164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition.	N/A	H-CIS-NEXU-180220/1165

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_9364c					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could	N/A	H-CIS-NEXU-180220/1166

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an	N/A	H-CIS-NEXU-180220/1167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_9372px					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to	N/A	H-CIS-NEXU-180220/1168

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker	N/A	H-CIS-NEXU-180220/1169

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_9372px-e					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the	N/A	H-CIS-NEXU-180220/1170

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**	N/A	H-CIS-NEXU-180220/1171
nexus_9372tx					
Out-of-bounds	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol	N/A	H-CIS-NEXU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		180220/1172
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an	N/A	H-CIS-NEXU-180220/1173

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_9372tx-e					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco	N/A	H-CIS-NEXU-180220/1174

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery	N/A	H-CIS-NEXU-180220/1175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_9396px					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected	N/A	H-CIS-NEXU-180220/1176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory,	N/A	H-CIS-NEXU-180220/1177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_9396tx					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery	N/A	H-CIS-NEXU-180220/1178

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2	N/A	H-CIS-NEXU-180220/1179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			adjacent). **CVE ID : CVE-2020-3120**		
nexus_9504					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**	N/A	H-CIS-NEXU-180220/1180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**	N/A	H-CIS-NEXU-180220/1181
nexus_9508					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated,	N/A	H-CIS-NEXU-180220/1182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device,	N/A	H-CIS-NEXU-180220/1183

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_9516					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a	N/A	H-CIS-NEXU-180220/1184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a	N/A	H-CIS-NEXU-180220/1185

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_3016					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack	N/A	H-CIS-NEXU-180220/1186

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2	N/A	H-CIS-NEXU-180220/1187

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_3048					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker	N/A	H-CIS-NEXU-180220/1188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**	N/A	H-CIS-NEXU-180220/1189
nexus_3064					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**	N/A	H-CIS-NEXU-180220/1190
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS	N/A	H-CIS-NEXU-180220/1191

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_3064-t					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The	N/A	H-CIS-NEXU-180220/1192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the	N/A	H-CIS-NEXU-180220/1193

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_31108pc-v					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious	N/A	H-CIS-NEXU-180220/1194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could	N/A	H-CIS-NEXU-180220/1195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
nexus_31108tc-v					
Out-of-bounds Write	05-02-2020	8.3	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative	N/A	H-CIS-NEXU-180220/1196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3119**		
Integer Overflow or Wraparound	05-02-2020	6.1	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the	N/A	H-CIS-NEXU-180220/1197

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device (Layer 2 adjacent). **CVE ID : CVE-2020-3120**		
Digi					
transport_wr21					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-02-2020	3.5	Digi TransPort WR21 5.2.2.3, WR44 5.1.6.4, and WR44v2 5.1.6.9 devices allow stored XSS in the web application. **CVE ID : CVE-2020-8822**	N/A	H-DIG-TRAN-180220/1198
transport_wr44					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-02-2020	3.5	Digi TransPort WR21 5.2.2.3, WR44 5.1.6.4, and WR44v2 5.1.6.9 devices allow stored XSS in the web application. **CVE ID : CVE-2020-8822**	N/A	H-DIG-TRAN-180220/1199
Draytek					
vigor2960					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	01-02-2020	10	DrayTek Vigor2960 1.3.1_Beta, Vigor3900 1.4.4_Beta, and Vigor300B 1.3.3_Beta, 1.4.2.1_Beta, and 1.4.4_Beta devices allow remote code execution as root (without authentication) via shell metacharacters to the cgi-bin/mainfunction.cgi URI. This issue has been fixed in Vigor3900/2960/300B v1.5.1. **CVE ID : CVE-2020-8515**	N/A	H-DRA-VIGO-180220/1200

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
vigor300b					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	01-02-2020	10	DrayTek Vigor2960 1.3.1_Beta, Vigor3900 1.4.4_Beta, and Vigor300B 1.3.3_Beta, 1.4.2.1_Beta, and 1.4.4_Beta devices allow remote code execution as root (without authentication) via shell metacharacters to the cgi-bin/mainfunction.cgi URI. This issue has been fixed in Vigor3900/2960/300B v1.5.1. **CVE ID : CVE-2020-8515**	N/A	H-DRA-VIGO-180220/1201
vigor3900					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	01-02-2020	10	DrayTek Vigor2960 1.3.1_Beta, Vigor3900 1.4.4_Beta, and Vigor300B 1.3.3_Beta, 1.4.2.1_Beta, and 1.4.4_Beta devices allow remote code execution as root (without authentication) via shell metacharacters to the cgi-bin/mainfunction.cgi URI. This issue has been fixed in Vigor3900/2960/300B v1.5.1. **CVE ID : CVE-2020-8515**	N/A	H-DRA-VIGO-180220/1202
Microsoft					
surface_hub					
Incorrect Authorization	11-02-2020	4.6	A security feature bypass vulnerability exists in Surface Hub when prompting for credentials, aka 'Surface Hub Security Feature Bypass	N/A	H-MIC-SURF-180220/1203

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. **CVE ID : CVE-2020-0702**		
schmid-telecom					
zi_620_v400					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-02-2020	10	Schmid ZI 620 V400 VPN 090 routers allow an attacker to execute OS commands as root via shell metacharacters to an entry on the SSH subcommand menu, as demonstrated by ping. **CVE ID : CVE-2020-6760**	N/A	H-SCH-ZI_6-180220/1204