Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
adminpanel_project					
adminpanel					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-05-2020	7.5	Jason2605 AdminPanel 4.0 allows SQL Injection via the editPlayer.php hidden parameter. **CVE ID : CVE-2020-13433**	N/A	A-ADM-ADMI-010620/1
aegir_project					
aegir					
Information Exposure	27-05-2020	5	In AEgir greater than or equal to 21.7.0 and less than 21.10.1, aegir publish and aegir build may leak secrets from environment variables in the browser bundle published to npm. This has been fixed in 21.10.1. **CVE ID : CVE-2020-11059**	https://github.com/ipfs/aegir/security/advisories/GHSA-qfcv-5whw-7pcw	A-AEG-AEGI-010620/2
alberta					
abtracetogether					
N/A	18-05-2020	7.5	OpenTrace, as used in COVIDSafe through v1.0.17, TraceTogether, ABTraceTogether, and other applications on iOS and Android, allows remote attackers to conduct long-term re-identification	N/A	A-ALB-ABTR-010620/3

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks and possibly have unspecified other impact, because of how Bluetooth is used. **CVE ID : CVE-2020-12856**		
Apache					
couchdb					
Improper Privilege Management	20-05-2020	6.8	CouchDB version 3.0.0 shipped with a new configuration setting that governs access control to the entire database server called `require_valid_user_except_for_up`. It was meant as an extension to the long standing setting `require_valid_user`, which in turn requires that any and all requests to CouchDB will have to be made with valid credentials, effectively forbidding any anonymous requests. The new `require_valid_user_except_for_up` is an off-by-default setting that was meant to allow requiring valid credentials for all endpoints except for the `/_up` endpoint. However, the implementation of this made an error that lead to not enforcing credentials on any endpoint, when enabled. CouchDB versions 3.0.1[1] and 3.1.0[2] fix this issue. **CVE ID : CVE-2020-1955**	N/A	A-APA-COUC-010620/4

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
tomcat					
Deserialization of Untrusted Data	20-05-2020	6.8	When using Apache Tomcat versions 10.0.0-M1 to 10.0.0-M4, 9.0.0.M1 to 9.0.34, 8.5.0 to 8.5.54 and 7.0.0 to 7.0.103 if a) an attacker is able to control the contents and name of a file on the server; and b) the server is configured to use the PersistenceManager with a FileStore; and c) the PersistenceManager is configured with sessionAttributeValueClass NameFilter="null" (the default unless a SecurityManager is used) or a sufficiently lax filter to allow the attacker provided object to be deserialized; and d) the attacker knows the relative file path from the storage location used by FileStore to the file the attacker has control over; then, using a specifically crafted request, the attacker will be able to trigger remote code execution via deserialization of the file under their control. Note that all of conditions a) to d) must be true for the attack to succeed. **CVE ID : CVE-2020-9484**	https://security.netapp.com/advisory/ntap-20200528-0005/	A-APA-TOMC-010620/5
kylin					
Improper Neutralization of Special	22-05-2020	9	Kylin has some restful apis which will concatenate os command with the user	N/A	A-APA-KYLI-010620/6

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			input string, a user is likely to be able to execute any os command without any protection or validation. **CVE ID : CVE-2020-1956**		
avantfax					
avantfax					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-05-2020	6.5	sendfax.php in iFAX AvantFAX before 3.3.6 and HylaFAX Enterprise Web Interface before 0.2.5 allows authenticated Command Injection. **CVE ID : CVE-2020-11766**	ftp://ftp.ifax.com/security/CVE-2020-11766.html	A-AVA-AVAN-010620/7
aviatrix					
controller					
Cross-Site Request Forgery (CSRF)	22-05-2020	6.8	An issue was discovered in Aviatrix Controller before 5.4.1204. An API call on the web interface lacked a session token check to control access, leading to CSRF. **CVE ID : CVE-2020-13412**	N/A	A-AVI-CONT-010620/8
Information Exposure	22-05-2020	5	An issue was discovered in Aviatrix Controller before 5.4.1204. There is a Observable Response Discrepancy from the API, which makes it easier to perform user enumeration via brute force. **CVE ID : CVE-2020-13413**	N/A	A-AVI-CONT-010620/9
Insufficiently Protected Credentials	22-05-2020	5	An issue was discovered in Aviatrix Controller before 5.4.1204. It contains credentials unused by the	N/A	A-AVI-CONT-010620/10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			software. **CVE ID : CVE-2020-13414**		
Improper Verification of Cryptographic Signature	22-05-2020	5	An issue was discovered in Aviatrix Controller through 5.1. An attacker with any signed SAML assertion from the Identity Provider can establish a connection (even if that SAML assertion has expired or is from a user who is not authorized to access Aviatrix), aka XML Signature Wrapping. **CVE ID : CVE-2020-13415**	N/A	A-AVI-CONT-010620/11
Cross-Site Request Forgery (CSRF)	22-05-2020	4.3	An issue was discovered in Aviatrix Controller before 5.4.1066. A Controller Web Interface session token parameter is not required on an API call, which opens the application up to a Cross Site Request Forgery (CSRF) vulnerability for password resets. **CVE ID : CVE-2020-13416**	N/A	A-AVI-CONT-010620/12
Improper Privilege Management	22-05-2020	7.5	An Elevation of Privilege issue was discovered in Aviatrix VPN Client before 2.10.7, because of an incomplete fix for CVE-2020-7224. This affects Linux, macOS, and Windows installations for certain OpenSSL parameters. **CVE ID : CVE-2020-13417**	N/A	A-AVI-CONT-010620/13
gateway					
Insufficiently Protected	22-05-2020	5	An issue was discovered in Aviatrix Controller before	N/A	A-AVI-GATE-010620/14

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			5.4.1204. It contains credentials unused by the software. **CVE ID : CVE-2020-13414**		
Improper Privilege Management	22-05-2020	7.5	An Elevation of Privilege issue was discovered in Aviatrix VPN Client before 2.10.7, because of an incomplete fix for CVE-2020-7224. This affects Linux, macOS, and Windows installations for certain OpenSSL parameters. **CVE ID : CVE-2020-13417**	N/A	A-AVI-GATE-010620/15
vpn_client					
Improper Privilege Management	22-05-2020	7.5	An Elevation of Privilege issue was discovered in Aviatrix VPN Client before 2.10.7, because of an incomplete fix for CVE-2020-7224. This affects Linux, macOS, and Windows installations for certain OpenSSL parameters. **CVE ID : CVE-2020-13417**	N/A	A-AVI-VPN_-010620/16
axel_project					
axel					
Improper Certificate Validation	26-05-2020	4.3	An issue was discovered in ssl.c in Axel before 2.17.8. The TLS implementation lacks hostname verification. **CVE ID : CVE-2020-13614**	N/A	A-AXE-AXEL-010620/17
Bbpress					
bbpress					
Improper Neutralization of Input During	26-05-2020	3.5	The bbPress plugin through 2.6.4 for WordPress has stored XSS in the Forum	N/A	A-BBP-BBPR-010620/18

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			creation section, resulting in JavaScript execution at wp-admin/edit.php?post_type=forum (aka the Forum listing page) for all users. An administrator can exploit this at the wp-admin/post.php?action=edit URI. **CVE ID : CVE-2020-13487**		
Improper Privilege Management	29-05-2020	7.5	An unauthenticated privilege-escalation issue exists in the bbPress plugin before 2.6.5 for WordPress when New User Registration is enabled. **CVE ID : CVE-2020-13693**	N/A	A-BBP-BBPR-010620/19
Bluetooth					
bluetooth_core					
Interpretation Conflict	19-05-2020	4.3	Pairing in Bluetooth® Core v5.2 and earlier may permit an unauthenticated attacker to acquire credentials with two pairing devices via adjacent access when the unauthenticated user initiates different pairing methods in each peer device and an end-user erroneously completes both pairing procedures with the MITM using the confirmation number of one peer as the passkey of the other. An adjacent, unauthenticated attacker could be able to initiate any Bluetooth operation on	https://www.bluetooth.com/learn-about-bluetooth/bluetooth-technology/bluetooth-security/method-vulnerability/	A-BLU-BLUE-010620/20

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			either attacked device exposed by the enabled Bluetooth profiles. This exposure may be limited when the user must authorize certain access explicitly, but so long as a user assumes that it is the intended remote device requesting permissions, device-local protections may be weakened. **CVE ID : CVE-2020-10134**		
Improper Authentication	19-05-2020	4.8	Legacy pairing and secure-connections pairing authentication in BluetoothÂ® BR/EDR Core Specification v5.2 and earlier may allow an unauthenticated user to complete authentication without pairing credentials via adjacent access. An unauthenticated, adjacent attacker could impersonate a Bluetooth BR/EDR master or slave to pair with a previously paired remote device to successfully complete the authentication procedure without knowing the link key. **CVE ID : CVE-2020-10135**	https://www.bluetooth.com/learn-about-bluetooth/bluetooth-technology/bluetooth-security/bias-vulnerability/	A-BLU-BLUE-010620/21
Cacti					
cacti					
Improper Preservation of Permissions	20-05-2020	4	In Cacti before 1.2.11, disabling a user account does not immediately invalidate any permissions	N/A	A-CAC-CACT-010620/22

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			granted to that account (e.g., permission to view logs). **CVE ID : CVE-2020-13230**		
Cross-Site Request Forgery (CSRF)	20-05-2020	4.3	In Cacti before 1.2.11, auth_profile.php?action=edit allows CSRF for an admin email change. **CVE ID : CVE-2020-13231**	N/A	A-CAC-CACT-010620/23
Centreon					
widget-host-monitoring					
Information Exposure	27-05-2020	3.3	Centreon before 19.10.7 exposes Session IDs in server responses. **CVE ID : CVE-2020-10945**	N/A	A-CEN-WIDG-010620/24
centreon_host-monitoring_widget					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-05-2020	4.3	Cross-site scripting (XSS) vulnerability allows remote attackers to inject arbitrary web script or HTML via the page parameter to service-monitoring/src/index.php. This vulnerability is fixed in versions 1.6.4, 18.10.3, 19.04.3, and 19.0.1 of the Centreon host-monitoring widget; 1.6.4, 18.10.5, 19.04.3, 19.10.2 of the Centreon service-monitoring widget; and 1.0.3, 18.10.1, 19.04.1, 19.10.1 of the Centreon tactical-overview widget. **CVE ID : CVE-2020-10946**	N/A	A-CEN-CENT-010620/25
Improper Neutralization of Input During Web Page	27-05-2020	4.3	Cross-site scripting (XSS) vulnerability allows remote attackers to inject arbitrary web script or HTML via the	N/A	A-CEN-CENT-010620/26

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			widgetId parameter to service-monitoring/src/index.php. This vulnerability is fixed in versions 1.6.4, 18.10.3, 19.04.3, and 19.0.1 of the Centreon host-monitoring widget; 1.6.4, 18.10.5, 19.04.3, 19.10.2 of the Centreon service-monitoring widget; and 1.0.3, 18.10.1, 19.04.1, 19.10.1 of the Centreon tactical-overview widget. **CVE ID : CVE-2020-13627**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-05-2020	4.3	Cross-site scripting (XSS) vulnerability allows remote attackers to inject arbitrary web script or HTML via the widgetId parameter to host-monitoring/src/toolbar.php . This vulnerability is fixed in versions 1.6.4, 18.10.3, 19.04.3, and 19.0.1 of the Centreon host-monitoring widget; 1.6.4, 18.10.5, 19.04.3, 19.10.2 of the Centreon service-monitoring widget; and 1.0.3, 18.10.1, 19.04.1, 19.10.1 of the Centreon tactical-overview widget. **CVE ID : CVE-2020-13628**	N/A	A-CEN-CENT-010620/27
centreon_tactical-overview_widget					
Improper Neutralization of Input During Web Page Generation ('Cross-site	27-05-2020	4.3	Cross-site scripting (XSS) vulnerability allows remote attackers to inject arbitrary web script or HTML via the page parameter to service-monitoring/src/index.php.	N/A	A-CEN-CENT-010620/28

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			This vulnerability is fixed in versions 1.6.4, 18.10.3, 19.04.3, and 19.0.1 of the Centreon host-monitoring widget; 1.6.4, 18.10.5, 19.04.3, 19.10.2 of the Centreon service-monitoring widget; and 1.0.3, 18.10.1, 19.04.1, 19.10.1 of the Centreon tactical-overview widget. **CVE ID : CVE-2020-10946**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-05-2020	4.3	Cross-site scripting (XSS) vulnerability allows remote attackers to inject arbitrary web script or HTML via the widgetId parameter to service-monitoring/src/index.php. This vulnerability is fixed in versions 1.6.4, 18.10.3, 19.04.3, and 19.0.1 of the Centreon host-monitoring widget; 1.6.4, 18.10.5, 19.04.3, 19.10.2 of the Centreon service-monitoring widget; and 1.0.3, 18.10.1, 19.04.1, 19.10.1 of the Centreon tactical-overview widget. **CVE ID : CVE-2020-13627**	N/A	A-CEN-CENT-010620/29
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-05-2020	4.3	Cross-site scripting (XSS) vulnerability allows remote attackers to inject arbitrary web script or HTML via the widgetId parameter to host-monitoring/src/toolbar.php . This vulnerability is fixed in versions 1.6.4, 18.10.3, 19.04.3, and 19.0.1 of the	N/A	A-CEN-CENT-010620/30

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Centreon host-monitoring widget; 1.6.4, 18.10.5, 19.04.3, 19.10.2 of the Centreon service-monitoring widget; and 1.0.3, 18.10.1, 19.04.1, 19.10.1 of the Centreon tactical-overview widget. **CVE ID : CVE-2020-13628**		
centreon_service-monitoring_widget					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-05-2020	4.3	Cross-site scripting (XSS) vulnerability allows remote attackers to inject arbitrary web script or HTML via the page parameter to service-monitoring/src/index.php. This vulnerability is fixed in versions 1.6.4, 18.10.3, 19.04.3, and 19.0.1 of the Centreon host-monitoring widget; 1.6.4, 18.10.5, 19.04.3, 19.10.2 of the Centreon service-monitoring widget; and 1.0.3, 18.10.1, 19.04.1, 19.10.1 of the Centreon tactical-overview widget. **CVE ID : CVE-2020-10946**	N/A	A-CEN-CENT-010620/31
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-05-2020	4.3	Cross-site scripting (XSS) vulnerability allows remote attackers to inject arbitrary web script or HTML via the widgetId parameter to service-monitoring/src/index.php. This vulnerability is fixed in versions 1.6.4, 18.10.3, 19.04.3, and 19.0.1 of the Centreon host-monitoring widget; 1.6.4, 18.10.5,	N/A	A-CEN-CENT-010620/32

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.04.3, 19.10.2 of the Centreon service-monitoring widget; and 1.0.3, 18.10.1, 19.04.1, 19.10.1 of the Centreon tactical-overview widget. **CVE ID : CVE-2020-13627**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-05-2020	4.3	Cross-site scripting (XSS) vulnerability allows remote attackers to inject arbitrary web script or HTML via the widgetId parameter to host-monitoring/src/toolbar.php . This vulnerability is fixed in versions 1.6.4, 18.10.3, 19.04.3, and 19.0.1 of the Centreon host-monitoring widget; 1.6.4, 18.10.5, 19.04.3, 19.10.2 of the Centreon service-monitoring widget; and 1.0.3, 18.10.1, 19.04.1, 19.10.1 of the Centreon tactical-overview widget. **CVE ID : CVE-2020-13628**	N/A	A-CEN-CENT-010620/33
centreon					
Information Exposure	27-05-2020	3.3	Centreon before 19.10.7 exposes Session IDs in server responses. **CVE ID : CVE-2020-10945**	N/A	A-CEN-CENT-010620/34
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-05-2020	9	Centreon before 19.04.15 allows remote attackers to execute arbitrary OS commands by placing shell metacharacters in RRDdatabase_status_path (via a main.get.php request) and then visiting the include/views/graphs/grap	N/A	A-CEN-CENT-010620/35

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			hStatus/displayServiceStatus.php page. **CVE ID : CVE-2020-13252**		
Cisco					
unified_contact_center_express					
Deserialization of Untrusted Data	22-05-2020	10	A vulnerability in the Java Remote Management Interface of Cisco Unified Contact Center Express (Unified CCX) could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. The vulnerability is due to insecure deserialization of user-supplied content by the affected software. An attacker could exploit this vulnerability by sending a malicious serialized Java object to a specific listener on an affected system. A successful exploit could allow the attacker to execute arbitrary code as the root user on an affected device. **CVE ID : CVE-2020-3280**	N/A	A-CIS-UNIF-010620/36
prime_network_registrar					
Improper Input Validation	22-05-2020	7.8	A vulnerability in the DHCP server of Cisco Prime Network Registrar could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient input	N/A	A-CIS-PRIM-010620/37

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validation of incoming DHCP traffic. An attacker could exploit this vulnerability by sending a crafted DHCP request to an affected device. A successful exploit could allow the attacker to cause a restart of the DHCP server process, causing a DoS condition. **CVE ID : CVE-2020-3272**		
prime_collaboration_provisioning					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-05-2020	6.5	A vulnerability in the web-based management interface of Cisco Prime Collaboration Provisioning Software could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. The vulnerability exists because the web-based management interface improperly validates user input for specific SQL queries. An attacker could exploit this vulnerability by authenticating to the application with valid administrative credentials and sending malicious requests to an affected system. A successful exploit could allow the attacker to view information that they are not authorized to view, make changes to the system that they are not authorized to make, or delete	N/A	A-CIS-PRIM-010620/38

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information from the database that they are not authorized to delete. **CVE ID : CVE-2020-3184**		
advanced_malware_protection_for_endpoints					
Improper Input Validation	22-05-2020	5.8	A vulnerability in the file scan process of Cisco AMP for Endpoints Mac Connector Software could cause the scan engine to crash during the scan of local files, resulting in a restart of the AMP Connector and a denial of service (DoS) condition of the Cisco AMP for Endpoints service. The vulnerability is due to insufficient input validation of specific file attributes. An attacker could exploit this vulnerability by providing a crafted file to a user of an affected system. A successful exploit could allow the attacker to cause the Cisco AMP for Endpoints service to crash, resulting in missed detection and logging of the potentially malicious file. Continued attempts to scan the file could result in a DoS condition of the Cisco AMP for Endpoints service. **CVE ID : CVE-2020-3314**	N/A	A-CIS-ADVA-010620/39
Buffer Copy without Checking Size of Input	22-05-2020	2.1	A vulnerability in Cisco AMP for Endpoints Linux Connector Software and Cisco AMP for Endpoints	N/A	A-CIS-ADVA-010620/40

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Mac Connector Software could allow an authenticated, local attacker to cause a buffer overflow on an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted packet to an affected device. A successful exploit could allow the attacker to cause the Cisco AMP for Endpoints service to crash and restart. **CVE ID : CVE-2020-3343**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	2.1	A vulnerability in Cisco AMP for Endpoints Linux Connector Software and Cisco AMP for Endpoints Mac Connector Software could allow an authenticated, local attacker to cause a buffer overflow on an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted packet to an affected device. A successful exploit could allow the attacker to cause the Cisco AMP for Endpoints service to crash and restart. **CVE ID : CVE-2020-3344**	N/A	A-CIS-ADVA-010620/41
Cmsmadesimple					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
cms_made_simple					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-05-2020	3.5	CMS Made Simple through 2.2.14 allows XSS via a crafted File Picker profile name. **CVE ID : CVE-2020-13660**	N/A	A-CMS-CMS_-010620/42
contentful					
python_example					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-05-2020	4.3	Contentful through 2020-05-21 for Python allows reflected XSS, as demonstrated by the api parameter to the-example-app.py. **CVE ID : CVE-2020-13258**	N/A	A-CON-PYTH-010620/43
Cybozu					
desktop					
Improper Input Validation	25-05-2020	7.5	Cybozu Desktop for Windows 2.0.23 to 2.2.40 allows remote code execution via unspecified vectors. **CVE ID : CVE-2020-5537**	N/A	A-CYB-DESK-010620/44
mailwise					
Information Exposure	29-05-2020	2.1	Android App 'Mailwise for Android' 1.0.0 to 1.0.1 allows an attacker to obtain credential information registered in the product via unspecified vectors. **CVE ID : CVE-2020-5572**	N/A	A-CYB-MAIL-010620/45
kintone					
Information Exposure	29-05-2020	2.1	Android App 'kintone mobile for Android' 1.0.0 to 2.5 allows an attacker to	N/A	A-CYB-KINT-010620/46

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			obtain credential information registered in the product via unspecified vectors. **CVE ID : CVE-2020-5573**		
Dell					
emc_isilon_onefs					
Information Exposure	20-05-2020	5	Dell EMC Isilon OneFS versions 8.2.2 and earlier contain an SNMPv2 vulnerability. The SNMPv2 services is enabled, by default, with a pre-configured community string. This community string allows read-only access to many aspects of the Isilon cluster, some of which are considered sensitive and can foster additional access. **CVE ID : CVE-2020-5364**	N/A	A-DEL-EMC_-010620/47
Use of Insufficiently Random Values	20-05-2020	5	Dell EMC Isilon versions 8.2.2 and earlier contain a remotesupport vulnerability. The pre-configured support account, remotesupport, is bundled in the Dell EMC Isilon OneFS installation. This account is used for diagnostics and other support functions. Although the default password is different for every cluster, it is predictable. **CVE ID : CVE-2020-5365**	N/A	A-DEL-EMC_-010620/48
dext5					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
dext5					
Unrestricted Upload of File with Dangerous Type	25-05-2020	7.5	A Remote code execution vulnerability exists in DEXT5Upload in DEXT5 through 2.7.1402870. An attacker can upload a PHP file via dext5handler.jsp handler because the uploaded file is stored under dext5uploadeddata/. **CVE ID : CVE-2020-13442**	N/A	A-DEX-DEXT-010620/49
Dolibarr					
dolibarr					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-05-2020	3.5	The DMS/ECM module in Dolibarr 11.0.4 renders user-uploaded .html files in the browser when the attachment parameter is removed from the direct download link. This causes XSS. **CVE ID : CVE-2020-13239**	N/A	A-DOL-DOLI-010620/50
Incorrect Default Permissions	20-05-2020	5.5	The DMS/ECM module in Dolibarr 11.0.4 allows users with the 'Setup documents directories' permission to rename uploaded files to have insecure file extensions. This bypasses the .noexe protection mechanism against XSS. **CVE ID : CVE-2020-13240**	N/A	A-DOL-DOLI-010620/51
Improper Neutralization of Input During Web Page Generation ('Cross-site	18-05-2020	3.5	Dolibarr before 11.0.4 allows XSS. **CVE ID : CVE-2020-13094**	N/A	A-DOL-DOLI-010620/52

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')					
Dovecot					
dovecot					
NULL Pointer Dereference	18-05-2020	5	In Dovecot before 2.3.10.1, unauthenticated sending of malformed parameters to a NOOP command causes a NULL Pointer Dereference and crash in submission-login, submission, or lmtp. **CVE ID : CVE-2020-10957**	https://www.openwall.com/lists/oss-security/2020/05/18/1	A-DOV-DOVE-010620/53
Use After Free	18-05-2020	5	In Dovecot before 2.3.10.1, a crafted SMTP/LMTP message triggers an unauthenticated use-after-free bug in submission-login, submission, or lmtp, and can lead to a crash under circumstances involving many newlines after a command. **CVE ID : CVE-2020-10958**	https://www.openwall.com/lists/oss-security/2020/05/18/1	A-DOV-DOVE-010620/54
Improper Input Validation	18-05-2020	5	In Dovecot before 2.3.10.1, remote unauthenticated attackers can crash the lmtp or submission process by sending mail with an empty localpart. **CVE ID : CVE-2020-10967**	https://www.openwall.com/lists/oss-security/2020/05/18/1	A-DOV-DOVE-010620/55
dpdk					
data_plane_development_kit					
Integer Overflow or Wraparound	19-05-2020	4.6	A vulnerability was found in DPDK versions 18.05 and above. A missing check for an integer overflow in vhost_user_set_log_base() could result in a smaller memory map than	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-	A-DPD-DATA-010620/56

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			requested, possibly allowing memory corruption. **CVE ID : CVE-2020-10722**	10722	
Integer Overflow or Wraparound	19-05-2020	4.6	A memory corruption issue was found in DPDK versions 17.05 and above. This flaw is caused by an integer truncation on the index of a payload. Under certain circumstances, the index (a UInt) is copied and truncated into a uint16, which can lead to out of bound indexing and possible memory corruption. **CVE ID : CVE-2020-10723**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10723	A-DPD-DATA-010620/57
Integer Overflow or Wraparound	19-05-2020	2.1	A vulnerability was found in DPDK versions 18.11 and above. The vhost-crypto library code is missing validations for user-supplied values, potentially allowing an information leak through an out-of-bounds memory read. **CVE ID : CVE-2020-10724**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10724	A-DPD-DATA-010620/58
Improper Initialization	20-05-2020	4	A flaw was found in DPDK version 19.11 and above that allows a malicious guest to cause a segmentation fault of the vhost-user backend application running on the host, which could result in a loss of connectivity for the other guests running on that host. This is caused by	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10725	A-DPD-DATA-010620/59

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a missing validity check of the descriptor address in the function `virtio_dev_rx_batch_packed ()`. **CVE ID : CVE-2020-10725**		
Integer Overflow or Wraparound	20-05-2020	2.1	A vulnerability was found in DPDK versions 19.11 and above. A malicious container that has direct access to the vhost-user socket can keep sending VHOST_USER_GET_INFLIGHT_FD messages, causing a resource leak (file descriptors and virtual memory), which may result in a denial of service. **CVE ID : CVE-2020-10726**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10726	A-DPD-DATA-010620/60
druva					
insync_client					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-05-2020	7.2	Relative path traversal in Druva inSync Windows Client 6.6.3 allows a local, unauthenticated attacker to execute arbitrary operating system commands with SYSTEM privileges. **CVE ID : CVE-2020-5752**	N/A	A-DRU-INSY-010620/61
EDX					
open_edx_platform					
Improper Input Validation	18-05-2020	6.5	Studio in Open edX Ironwood 2.5, when CodeJail is not used, allows a user to go to the "Create New course>New section>New subsection>New unit>Add	N/A	A-EDX-OPEN-010620/62

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			new component>Problem button>Advanced tab>Custom Python evaluated code" screen, edit the problem, and execute Python code. This leads to arbitrary code execution. **CVE ID : CVE-2020-13144**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-05-2020	3.5	Studio in Open edX Ironwood 2.5 allows users to upload SVG files via the "Content>File Uploads" screen. These files can contain JavaScript code and thus lead to Stored XSS. **CVE ID : CVE-2020-13145**	N/A	A-EDX-OPEN-010620/63
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-05-2020	6.8	Studio in Open edX Ironwood 2.5 allows CSV injection because an added cohort in Course>Instructor>Cohorts may contain a formula that is exported via the "Course>Data Downloads>Reports>Download profile info" feature. **CVE ID : CVE-2020-13146**	N/A	A-EDX-OPEN-010620/64
elementor					
elementor					
Unrestricted Upload of File with Dangerous Type	17-05-2020	6.5	An issue was discovered in the Elementor Pro plugin before 2.9.4 for WordPress, as exploited in the wild in May 2020 in conjunction with CVE-2020-13125. An attacker with the Subscriber role can upload arbitrary executable files to achieve remote code	N/A	A-ELE-ELEM-010620/65

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. NOTE: the free Elementor plugin is unaffected. **CVE ID : CVE-2020-13126**		
em-http-request_project					
em-http-request					
Improper Certificate Validation	25-05-2020	6.8	EM-HTTP-Request 1.1.5 uses the library eventmachine in an insecure way that allows an attacker to perform a man-in-the-middle attack against users of the library. The hostname in a TLS server certificate is not verified. **CVE ID : CVE-2020-13482**	N/A	A-EM--EM-H-010620/66
em-imap_project					
em-imap					
Improper Certificate Validation	19-05-2020	5.8	em-imap 0.5 uses the library eventmachine in an insecure way that allows an attacker to perform a man-in-the-middle attack against users of the library. The hostname in a TLS server certificate is not verified. **CVE ID : CVE-2020-13163**	N/A	A-EM--EM-I-010620/67
Facebook					
proxygen					
Use After Free	18-05-2020	7.5	A use-after-free is possible due to an error in lifetime management in the request adaptor when a malicious client invokes request error handling in a specific sequence. This issue affects versions of proxygen prior	https://www.facebook.com/security/advisories/cve-2020-1897	A-FAC-PROX-010620/68

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to v2020.05.18.00. **CVE ID : CVE-2020-1897**		
ffjpeg_project					
ffjpeg					
Out-of-bounds Read	24-05-2020	4.3	ffjpeg through 2020-02-24 has an invalid read in jfif_encode in jfif.c. **CVE ID : CVE-2020-13438**	N/A	A-FFJ-FFJP-010620/69
Out-of-bounds Read	24-05-2020	4.3	ffjpeg through 2020-02-24 has a heap-based buffer over-read in jfif_decode in jfif.c. **CVE ID : CVE-2020-13439**	N/A	A-FFJ-FFJP-010620/70
Out-of-bounds Write	24-05-2020	4.3	ffjpeg through 2020-02-24 has an invalid write in bmp_load in bmp.c. **CVE ID : CVE-2020-13440**	N/A	A-FFJ-FFJP-010620/71
Fork-cms					
fork_cms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-05-2020	4.3	Fork before 5.8.3 allows XSS via navigation_title or title. **CVE ID : CVE-2020-13633**	N/A	A-FOR-FORK-010620/72
freerdp					
freerdp					
Double Free	29-05-2020	5	In FreeRDP less than or equal to 2.0.0, by providing manipulated input a malicious client can create a double free condition and crash the server. This is fixed in version 2.1.0. **CVE ID : CVE-2020-11017**	https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-q5c8-	A-FRE-FREE-010620/73

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				fm29-q57c	
Out-of-bounds Read	29-05-2020	4	In FreeRDP less than or equal to 2.0.0, a possible resource exhaustion vulnerability can be performed. Malicious clients could trigger out of bound reads causing memory allocation with random size. This has been fixed in 2.1.0. **CVE ID : CVE-2020-11018**	https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-8cvc-vcw7-6mfw	A-FRE-FREE-010620/74
Out-of-bounds Read	22-05-2020	2.1	An issue was discovered in FreeRDP before 2.1.1. An out-of-bounds (OOB) read vulnerability has been detected in ntlm_read_ChallengeMessage in winpr/libwinpr/sspi/NTLM/ntlm_message.c. **CVE ID : CVE-2020-13396**	N/A	A-FRE-FREE-010620/75
Out-of-bounds Read	22-05-2020	2.1	An issue was discovered in FreeRDP before 2.1.1. An out-of-bounds (OOB) read vulnerability has been detected in security_fips_decrypt in libfreerdp/core/security.c due to an uninitialized value. **CVE ID : CVE-2020-13397**	N/A	A-FRE-FREE-010620/76
Out-of-bounds Write	22-05-2020	2.1	An issue was discovered in FreeRDP before 2.1.1. An out-of-bounds (OOB) write vulnerability has been detected in crypto_rsa_common in	N/A	A-FRE-FREE-010620/77

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			libfreerdp/crypto/crypto.c. **CVE ID : CVE-2020-13398**		
gitea					
gitea					
Improper Locking	20-05-2020	5	An issue was discovered in Gitea through 1.11.5. An attacker can trigger a deadlock by initiating a transfer of a repository's ownership from one organization to another. **CVE ID : CVE-2020-13246**	N/A	A-GIT-GITE-010620/78
Gnome					
balsa					
Improper Certificate Validation	28-05-2020	6.4	In GNOME glib-networking through 2.64.2, the implementation of GTlsClientConnection skips hostname verification of the server's TLS certificate if the application fails to specify the expected server identity. This is in contrast to its intended documented behavior, to fail the certificate verification. Applications that fail to provide the server identity, including Balsa before 2.5.11 and 2.6.x before 2.6.1, accept a TLS certificate if the certificate is valid for any host. **CVE ID : CVE-2020-13645**	N/A	A-GNO-BALS-010620/79
glib-networking					
Improper Certificate	28-05-2020	6.4	In GNOME glib-networking through 2.64.2, the implementation of	N/A	A-GNO-GLIB-010620/80

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			GTlsClientConnection skips hostname verification of the server's TLS certificate if the application fails to specify the expected server identity. This is in contrast to its intended documented behavior, to fail the certificate verification. Applications that fail to provide the server identity, including Balsa before 2.5.11 and 2.6.x before 2.6.1, accept a TLS certificate if the certificate is valid for any host. **CVE ID : CVE-2020-13645**		
gonitro					
nitro_pro					
Integer Overflow or Wraparound	18-05-2020	6.8	An exploitable code execution vulnerability exists in the way Nitro Pro 13.9.1.155 parses Pattern objects. A specially crafted PDF file can trigger an integer overflow that can lead to arbitrary code execution. In order to trigger this vulnerability, victim must open a malicious file. **CVE ID : CVE-2020-6092**	N/A	A-GON-NITR-010620/81
Access of Uninitialized Pointer	18-05-2020	4.3	An exploitable information disclosure vulnerability exists in the way Nitro Pro 13.9.1.155 does XML error handling. A specially crafted PDF document can cause uninitialized memory	N/A	A-GON-NITR-010620/82

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access resulting in information disclosure. In order to trigger this vulnerability, victim must open a malicious file. **CVE ID : CVE-2020-6093**		
Use After Free	18-05-2020	6.8	An exploitable code execution vulnerability exists in the PDF parser of Nitro Pro 13.9.1.155. A specially crafted PDF document can cause a use-after-free which can lead to remote code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2020-6074**	N/A	A-GON-NITR-010620/83
Google					
chrome					
Access of Resource Using Incompatible Type ('Type Confusion')	21-05-2020	6.8	Type confusion in V8 in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6468**	N/A	A-GOO-CHRO-010620/84
Incorrect Default Permissions	21-05-2020	6.8	Insufficient policy enforcement in developer tools in Google Chrome prior to 83.0.4103.61 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension.	N/A	A-GOO-CHRO-010620/85

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-6469		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-05-2020	4.3	Insufficient validation of untrusted input in clipboard in Google Chrome prior to 83.0.4103.61 allowed a local attacker to inject arbitrary scripts or HTML (UXSS) via crafted clipboard contents. **CVE ID : CVE-2020-6470**	N/A	A-GOO-CHRO-010620/86
Incorrect Default Permissions	21-05-2020	6.8	Insufficient policy enforcement in developer tools in Google Chrome prior to 83.0.4103.61 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension. **CVE ID : CVE-2020-6471**	N/A	A-GOO-CHRO-010620/87
Information Exposure	21-05-2020	4.3	Insufficient policy enforcement in developer tools in Google Chrome prior to 83.0.4103.61 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information from process memory or disk via a crafted Chrome Extension. **CVE ID : CVE-2020-6472**	N/A	A-GOO-CHRO-010620/88
Information Exposure	21-05-2020	4.3	Insufficient policy enforcement in Blink in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to obtain potentially sensitive	N/A	A-GOO-CHRO-010620/89

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information from process memory via a crafted HTML page. **CVE ID : CVE-2020-6473**		
Use After Free	21-05-2020	6.8	Use after free in Blink in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6474**	N/A	A-GOO-CHRO-010620/90
N/A	21-05-2020	4.3	Incorrect implementation in full screen in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to spoof security UI via a crafted HTML page. **CVE ID : CVE-2020-6475**	N/A	A-GOO-CHRO-010620/91
Incorrect Default Permissions	21-05-2020	4.3	Insufficient policy enforcement in tab strip in Google Chrome prior to 83.0.4103.61 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension. **CVE ID : CVE-2020-6476**	N/A	A-GOO-CHRO-010620/92
Improper Privilege Management	21-05-2020	6.8	Inappropriate implementation in installer in Google Chrome on OS X prior to 83.0.4103.61 allowed a local attacker to perform privilege escalation via a crafted file. **CVE ID : CVE-2020-6477**	N/A	A-GOO-CHRO-010620/93

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	21-05-2020	4.3	Inappropriate implementation in full screen in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to spoof security UI via a crafted HTML page. **CVE ID : CVE-2020-6478**	N/A	A-GOO-CHRO-010620/94
N/A	21-05-2020	4.3	Inappropriate implementation in sharing in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to spoof security UI via a crafted HTML page. **CVE ID : CVE-2020-6479**	N/A	A-GOO-CHRO-010620/95
Incorrect Default Permissions	21-05-2020	1.9	Insufficient policy enforcement in enterprise in Google Chrome prior to 83.0.4103.61 allowed a local attacker to bypass navigation restrictions via UI actions. **CVE ID : CVE-2020-6480**	N/A	A-GOO-CHRO-010620/96
N/A	21-05-2020	4.3	Insufficient policy enforcement in URL formatting in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to perform domain spoofing via a crafted domain name. **CVE ID : CVE-2020-6481**	N/A	A-GOO-CHRO-010620/97
Incorrect Default Permissions	21-05-2020	4.3	Insufficient policy enforcement in developer tools in Google Chrome prior to 83.0.4103.61 allowed an attacker who convinced a user to install a	N/A	A-GOO-CHRO-010620/98

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious extension to bypass navigation restrictions via a crafted Chrome Extension. **CVE ID : CVE-2020-6482**		
Incorrect Default Permissions	21-05-2020	4.3	Insufficient policy enforcement in payments in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. **CVE ID : CVE-2020-6483**	N/A	A-GOO-CHRO-010620/99
Incorrect Default Permissions	21-05-2020	4.3	Insufficient data validation in ChromeDriver in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to bypass navigation restrictions via a crafted request. **CVE ID : CVE-2020-6484**	N/A	A-GOO-CHRO-010620/100
Improper Input Validation	21-05-2020	4.3	Insufficient data validation in media router in Google Chrome prior to 83.0.4103.61 allowed a remote attacker who had compromised the renderer process to bypass navigation restrictions via a crafted HTML page. **CVE ID : CVE-2020-6485**	N/A	A-GOO-CHRO-010620/101
N/A	21-05-2020	4.3	Insufficient policy enforcement in navigations in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	N/A	A-GOO-CHRO-010620/102

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-6486		
Incorrect Default Permissions	21-05-2020	4.3	Insufficient policy enforcement in downloads in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. **CVE ID : CVE-2020-6487**	N/A	A-GOO-CHRO-010620/103
Incorrect Default Permissions	21-05-2020	4.3	Insufficient policy enforcement in downloads in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. **CVE ID : CVE-2020-6488**	N/A	A-GOO-CHRO-010620/104
Information Exposure	21-05-2020	4.3	Inappropriate implementation in developer tools in Google Chrome prior to 83.0.4103.61 allowed a remote attacker who had convinced the user to take certain actions in developer tools to obtain potentially sensitive information from disk via a crafted HTML page. **CVE ID : CVE-2020-6489**	N/A	A-GOO-CHRO-010620/105
Exposure of Resource to Wrong Sphere	21-05-2020	4.3	Insufficient data validation in loader in Google Chrome prior to 83.0.4103.61 allowed a remote attacker who had been able to write to disk to leak cross-origin data via a crafted HTML page.	N/A	A-GOO-CHRO-010620/106

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-6490		
N/A	21-05-2020	4.3	Insufficient data validation in site information in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to spoof security UI via a crafted domain name. **CVE ID : CVE-2020-6491**	N/A	A-GOO-CHRO-010620/107
Use After Free	21-05-2020	6.8	Use after free in speech recognizer in Google Chrome prior to 81.0.4044.113 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. **CVE ID : CVE-2020-6457**	N/A	A-GOO-CHRO-010620/108
Out-of-bounds Write	21-05-2020	6.8	Out of bounds read and write in PDFium in Google Chrome prior to 81.0.4044.122 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. **CVE ID : CVE-2020-6458**	N/A	A-GOO-CHRO-010620/109
Use After Free	21-05-2020	6.8	Use after free in payments in Google Chrome prior to 81.0.4044.122 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6459**	N/A	A-GOO-CHRO-010620/110
N/A	21-05-2020	4.3	Insufficient data validation in URL formatting in Google Chrome prior to	N/A	A-GOO-CHRO-010620/111

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			81.0.4044.122 allowed a remote attacker to perform domain spoofing via a crafted domain name. **CVE ID : CVE-2020-6460**		
Use After Free	21-05-2020	6.8	Use after free in storage in Google Chrome prior to 81.0.4044.129 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. **CVE ID : CVE-2020-6461**	N/A	A-GOO-CHRO-010620/112
Use After Free	21-05-2020	6.8	Use after free in task scheduling in Google Chrome prior to 81.0.4044.129 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. **CVE ID : CVE-2020-6462**	N/A	A-GOO-CHRO-010620/113
Use After Free	21-05-2020	6.8	Use after free in ANGLE in Google Chrome prior to 81.0.4044.122 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6463**	N/A	A-GOO-CHRO-010620/114
Access of Resource Using Incompatible Type ('Type Confusion')	21-05-2020	6.8	Type confusion in Blink in Google Chrome prior to 81.0.4044.138 allowed a remote attacker to potentially exploit heap corruption via a crafted	N/A	A-GOO-CHRO-010620/115

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HTML page. **CVE ID : CVE-2020-6464**		
Use After Free	21-05-2020	6.8	Use after free in reader mode in Google Chrome on Android prior to 83.0.4103.61 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. **CVE ID : CVE-2020-6465**	N/A	A-GOO-CHRO-010620/116
Use After Free	21-05-2020	6.8	Use after free in media in Google Chrome prior to 83.0.4103.61 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. **CVE ID : CVE-2020-6466**	N/A	A-GOO-CHRO-010620/117
Use After Free	21-05-2020	6.8	Use after free in WebRTC in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6467**	N/A	A-GOO-CHRO-010620/118
grafana					
piechart-panel					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-05-2020	3.5	legend.ts in the piechart-panel (aka Pie Chart Panel) plugin before 1.5.0 for Grafana allows XSS via the Values Header (aka legend header) option.	N/A	A-GRA-PIEC-010620/119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-13429		
grafana					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-05-2020	4.3	Grafana before 7.0.0 allows tag value XSS via the OpenTSDB datasource. **CVE ID : CVE-2020-13430**	https://security.netapp.com/advisory/ntap-20200528-0003/	A-GRA-GRAF-010620/120
gwtupload_project					
gwtupload					
Unrestricted Upload of File with Dangerous Type	18-05-2020	5	An issue was discovered in Manolo GWTUpload 1.0.3. server/UploadServlet.java (the servlet for handling file upload) accepts a delay parameter that causes a thread to sleep. It can be abused to cause all of a server's threads to sleep, leading to denial of service. **CVE ID : CVE-2020-13128**	N/A	A-GWT-GWTU-010620/121
Health					
covidsafe					
N/A	18-05-2020	7.5	OpenTrace, as used in COVIDSafe through v1.0.17, TraceTogether, ABTraceTogether, and other applications on iOS and Android, allows remote attackers to conduct long-term re-identification attacks and possibly have unspecified other impact, because of how Bluetooth is used. **CVE ID : CVE-2020-12856**	N/A	A-HEA-COVI-010620/122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	18-05-2020	5	Caching of GATT characteristic values (TempID) in COVIDSafe v1.0.15 and v1.0.16 allows a remote attacker to long-term re-identify an Android device running COVIDSafe. **CVE ID : CVE-2020-12857**	N/A	A-HEA-COVI-010620/123
Improper Initialization	18-05-2020	5	Non-reinitialisation of random data in the advertising payload in COVIDSafe v1.0.15 and v1.0.16 allows a remote attacker to re-identify Android devices running COVIDSafe by scanning for their advertising beacons. **CVE ID : CVE-2020-12858**	N/A	A-HEA-COVI-010620/124
Cleartext Storage of Sensitive Information	18-05-2020	5	Unnecessary fields in the OpenTrace/BlueTrace protocol in COVIDSafe through v1.0.17 allow a remote attacker to identify a device model by observing cleartext payload data. This allows re-identification of devices, especially less common phone models or those in low-density situations. **CVE ID : CVE-2020-12859**	N/A	A-HEA-COVI-010620/125
Information Exposure	18-05-2020	5	COVIDSafe through v1.0.17 allows a remote attacker to access phone name and model information because a BLE device can have four roles and COVIDSafe uses all of them. This allows for re-identification of a device,	N/A	A-HEA-COVI-010620/126

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and potentially identification of the owner's name. **CVE ID : CVE-2020-12860**		
heinekingmedia					
stashcat					
Information Exposure	18-05-2020	9	An issue was discovered in the stashcat app through 3.9.1 for macOS, Windows, Android, iOS, and possibly other platforms. The GET method is used with client_key and device_id data in the query string, which allows attackers to obtain sensitive information by reading web-server logs. **CVE ID : CVE-2020-13129**	N/A	A-HEI-STAS-010620/127
hive					
netius					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	21-05-2020	4.3	netius prior to 1.17.58 is vulnerable to HTTP Request Smuggling. HTTP pipelining issues and request smuggling attacks might be possible due to incorrect Transfer encoding header parsing which could allow for CL:TE or TE:TE attacks. **CVE ID : CVE-2020-7655**	N/A	A-HIV-NETI-010620/128
Horde					
groupware					
Improper Neutralization of Input During Web Page Generation	18-05-2020	4.3	Gollem before 3.0.13, as used in Horde Groupware Webmail Edition 5.2.22 and other products, is affected by a reflected Cross-Site	https://github.com/horde/gollem/blob/95b2a4	A-HOR-GROU-010620/129

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Scripting (XSS) vulnerability via the HTTP GET dir parameter in the browser functionality, affecting breadcrumb output. An attacker can obtain access to a victim's webmail account by making them visit a malicious URL. **CVE ID : CVE-2020-8034**	212d734f1b27aaa7a221d2fa1370d2631f/docs/CHANGES, https://lists.horde.org/archives/gollem/Week-of-Mon-20200420/001990.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-05-2020	4.3	The image view functionality in Horde Groupware Webmail Edition before 5.2.22 is affected by a stored Cross-Site Scripting (XSS) vulnerability via an SVG image upload containing a JavaScript payload. An attacker can obtain access to a victim's webmail account by making them visit a malicious URL. **CVE ID : CVE-2020-8035**	https://github.com/horde/base/blob/c00f2fdb222055fb2ccb6d53b5b5240c0a7d2a75/docs/CHANGES, https://lists.horde.org/archives/announce/2020/001290.html	A-HOR-GROU-010620/130
gollem					
Improper Neutralization of Input During Web Page Generation	18-05-2020	4.3	Gollem before 3.0.13, as used in Horde Groupware Webmail Edition 5.2.22 and other products, is affected by a reflected Cross-Site	https://github.com/horde/gollem/blob/95b2a4	A-HOR-GOLL-010620/131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Scripting (XSS) vulnerability via the HTTP GET dir parameter in the browser functionality, affecting breadcrumb output. An attacker can obtain access to a victim's webmail account by making them visit a malicious URL. **CVE ID : CVE-2020-8034**	212d734f1b27aaa7a221d2fa1370d2631f/docs/CHANGES, https://lists.horde.org/archives/golle m/Week-of-Mon-20200420/001990.html	
httplib2_project					
httplib2					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-05-2020	4.3	In httplib2 before version 0.18.0, an attacker controlling unescaped part of uri for `httplib2.Http.request()` could change request headers and body, send additional hidden requests to same server. This vulnerability impacts software that uses httplib2 with uri constructed by string concatenation, as opposed to proper urllib building with escaping. This has been fixed in 0.18.0. **CVE ID : CVE-2020-11078**	https://github.com/httplib2/httplib2/security/advisories/GHSA-gg84-qgv9-w4pq	A-HTT-HTTP-010620/132
IBM					
mobilefirst_platform_foundation					
Information Exposure	27-05-2020	5	IBM MobileFirst Platform Foundation 8.0.0.0 stores	https://www.ibm.c	A-IBM-MOBI-010620/133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			highly sensitive information in URL parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referrer header or browser history. IBM X-Force ID: 175207. **CVE ID : CVE-2020-4226**	om/support/pages/node/6216813	
security_identity_governance_and_intelligence					
Improper Input Validation	28-05-2020	4	IBM Security Identity Governance and Intelligence 5.2.6 could allow an authenticated user to perform unauthorized commands due to hazardous input validation. IBM X-Force ID: 175335. **CVE ID : CVE-2020-4231**	https://www.ibm.com/support/pages/node/6207905	A-IBM-SECU-010620/134
Insufficiently Protected Credentials	28-05-2020	5	IBM Security Identity Governance and Intelligence 5.2.6 could allow an attacker to enumerate usernames to find valid login credentials which could be used to attempt further attacks against the system. IBM X-Force ID: 175336. **CVE ID : CVE-2020-4232**	https://www.ibm.com/support/pages/node/6207906	A-IBM-SECU-010620/135
Information Exposure	28-05-2020	5	IBM Security Identity Governance and Intelligence 5.2.6 could allow a remote attacker to obtain sensitive information, caused by the failure to set the secure flag for the session cookie in SSL	https://www.ibm.com/support/pages/node/6207912	A-IBM-SECU-010620/136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mode. By intercepting its transmission within an HTTP session, an attacker could exploit this vulnerability to capture the cookie and obtain sensitive information. IBM X-Force ID: 175360. **CVE ID : CVE-2020-4233**		
Information Exposure	28-05-2020	5	IBM Security Identity Governance and Intelligence 5.2.6 could allow an unauthorized user to obtain sensitive information through user enumeration. IBM X-Force ID: 175422. **CVE ID : CVE-2020-4244**	https://www.ibm.com/support/pages/node/6207907	A-IBM-SECU-010620/137
Weak Password Requirements	28-05-2020	5	IBM Security Identity Governance and Intelligence 5.2.6 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 175423. **CVE ID : CVE-2020-4245**	https://www.ibm.com/support/pages/node/6207908	A-IBM-SECU-010620/138
Improper Restriction of XML External Entity Reference ('XXE')	28-05-2020	5.5	IBM Security Identity Governance and Intelligence 5.2.6 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume	https://www.ibm.com/support/pages/node/6207902	A-IBM-SECU-010620/139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory resources. IBM X-Force ID: 175481. **CVE ID : CVE-2020-4246**		
Information Exposure	28-05-2020	4	IBM Security Identity Governance and Intelligence 5.2.6 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 175484. **CVE ID : CVE-2020-4248**	https://www.ibm.com/support/pages/node/6207913	A-IBM-SECU-010620/140
Information Exposure	28-05-2020	4	IBM Security Identity Governance and Intelligence 5.2.6 could disclose highly sensitive information to other authenticated users on the sytem due to incorrect authorization. IBM X-Force ID: 175485. **CVE ID : CVE-2020-4249**	https://www.ibm.com/support/pages/node/6207911	A-IBM-SECU-010620/141
planning_analytics_local					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-05-2020	3.5	IBM Planning Analytics Local 2.0.0 through 2.0.9 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 176735.	https://www.ibm.com/support/pages/node/6213263	A-IBM-PLAN-010620/142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-4306		
mq_for_hpe_nonstop					
Improper Privilege Management	29-05-2020	4.4	IBM MQ on HPE NonStop 8.0.4 and 8.1.0 is vulnerable to a privilege escalation attack when running in restricted mode. IBM X-Force ID: 178427. **CVE ID : CVE-2020-4352**	https://www.ibm.com/support/pages/node/6217600	A-IBM-MQ_F-010620/143
jazz_reporting_service					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-05-2020	3.5	IBM Jazz Reporting Service 6.0.6, 6.0.6.1, and 7.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 180071. **CVE ID : CVE-2020-4419**	https://www.ibm.com/support/pages/node/6217403	A-IBM-JAZZ-010620/144
spectrum_scale					
Incorrect Authorization	27-05-2020	4	IBM Spectrum Scale 4.2.0.0 through 4.2.3.21 and 5.0.0.0 through 5.0.4.4 could allow an authenticated GUI user to perform unauthorized actions due to missing function level access control. IBM X-Force ID: 178414 **CVE ID : CVE-2020-4348**	https://www.ibm.com/support/pages/node/6213739	A-IBM-SPEC-010620/145
Use of a Broken or Risky Cryptographic	27-05-2020	5	IBM Spectrum Scale 5.0.0.0 through 5.0.4.4 uses weaker than expected cryptographic algorithms	https://www.ibm.com/support/pages	A-IBM-SPEC-010620/146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Algorithm			that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 178423. **CVE ID : CVE-2020-4349**	/node/6214482	
Use of a Broken or Risky Cryptographic Algorithm	27-05-2020	5	IBM Spectrum Scale 5.0.0.0 through 5.0.4.4 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 178424. **CVE ID : CVE-2020-4350**	https://www.ibm.com/support/pages/node/6214480	A-IBM-SPEC-010620/147
Information Exposure	27-05-2020	4	IBM Spectrum Scale 5.0.0.0 through 5.0.4.4 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 178761. **CVE ID : CVE-2020-4357**	https://www.ibm.com/support/pages/node/6214478	A-IBM-SPEC-010620/148
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-05-2020	3.5	IBM Spectrum Scale 5.0.0.0 through 5.0.4.4 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 178762. **CVE ID : CVE-2020-4358**	https://www.ibm.com/support/pages/node/6214481	A-IBM-SPEC-010620/149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	27-05-2020	4	IBM Spectrum Scale 5.0.0.0 through 5.0.4.4 could allow a privileged authenticated user to perform unauthorized actions using a specially crated HTTP POST command. IBM X-Force ID: 179157. **CVE ID : CVE-2020-4378**	https://www.ibm.com/support/pages/node/6214484	A-IBM-SPEC-010620/150
Use of a Broken or Risky Cryptographic Algorithm	27-05-2020	5	IBM Spectrum Scale 5.0.0.0 through 5.0.4.4 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 179158. **CVE ID : CVE-2020-4379**	https://www.ibm.com/support/pages/node/6214483	A-IBM-SPEC-010620/151
Improper Input Validation	19-05-2020	4.9	The Spectrum Scale 4.2.0.0 through 4.2.3.21 and 5.0.0.0 through 5.0.4.3 file system component is affected by a denial of service vulnerability in its kernel module that could allow an attacker to cause a denial of service condition on the affected system. To exploit this vulnerability, a local attacker could invoke a subset of ioctls on the Spectrum Scale device with non-valid arguments. This could allow the attacker to crash the kernel. IBM X-Force ID: 179986. **CVE ID : CVE-2020-4411**	https://www.ibm.com/support/pages/node/6209002	A-IBM-SPEC-010620/152
N/A	19-05-2020	5	The Spectrum Scale 4.2.0.0 through 4.2.3.21 and 5.0.0.0	https://www.ibm.c	A-IBM-SPEC-010620/153

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			through 5.0.4.3 file system component is affected by a denial of service security vulnerability. An attacker can force the Spectrum Scale mmfsd/mmsdrserv daemons to unexpectedly exit, impacting the functionality of the Spectrum Scale cluster and the availability of file systems managed by Spectrum Scale. IBM X-Force ID: 179987. **CVE ID : CVE-2020-4412**	om/support/pages/node/6209004	
infosphere_information_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-05-2020	3.5	IBM InfoSphere Information Server 11.3, 11.5, and 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 176475. **CVE ID : CVE-2020-4298**	https://www.ibm.com/support/pages/node/6194775	A-IBM-INFO-010620/154
Cross-Site Request Forgery (CSRF)	19-05-2020	4.3	IBM InfoSphere Information Server 11.3, 11.5, and 11.7 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 176268. **CVE ID : CVE-2020-4286**	https://www.ibm.com/support/pages/node/6194751	A-IBM-INFO-010620/155

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
infosphere_information_server_on_cloud					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-05-2020	3.5	IBM InfoSphere Information Server 11.3, 11.5, and 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 176475. **CVE ID : CVE-2020-4298**	https://www.ibm.com/support/pages/node/6194775	A-IBM-INFO-010620/156
Cross-Site Request Forgery (CSRF)	19-05-2020	4.3	IBM InfoSphere Information Server 11.3, 11.5, and 11.7 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 176268. **CVE ID : CVE-2020-4286**	https://www.ibm.com/support/pages/node/6194751	A-IBM-INFO-010620/157
business_automation_workflow					
N/A	29-05-2020	5.8	IBM Business Automation Workflow 18 and 19, and IBM Business Process Manager 8.0, 8.5, and 8.6 could allow a remote attacker to bypass security restrictions, caused by a reverse tabnabbing flaw. An attacker could exploit this vulnerability and redirect a vitcim to a phishing site. IBM X-Force ID: 181989 **CVE ID : CVE-2020-4490**	https://www.ibm.com/support/pages/node/6217550	A-IBM-BUSI-010620/158

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
business_process_manager					
N/A	29-05-2020	5.8	IBM Business Automation Workflow 18 and 19, and IBM Business Process Manager 8.0, 8.5, and 8.6 could allow a remote attacker to bypass security restrictions, caused by a reverse tabnabbing flaw. An attacker could exploit this vulnerability and redirect a vitcim to a phishing site. IBM X-Force ID: 181989 **CVE ID : CVE-2020-4490**	https://www.ibm.com/support/pages/node/6217550	A-IBM-BUSI-010620/159
ifax					
hylafax					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-05-2020	6.5	sendfax.php in iFAX AvantFAX before 3.3.6 and HylaFAX Enterprise Web Interface before 0.2.5 allows authenticated Command Injection. **CVE ID : CVE-2020-11766**	ftp://ftp.ifax.com/security/CVE-2020-11766.html	A-IFA-HYLA-010620/160
infolific					
real-time_find_and_replace					
Cross-Site Request Forgery (CSRF)	28-05-2020	6.8	An issue was discovered in the Real-Time Find and Replace plugin before 4.0.2 for WordPress. The far_options_page function did not do any nonce verification, allowing for requests to be forged on behalf of an administrator. The find and replace rules could be updated with malicious JavaScript, allowing for that be	N/A	A-INF-REAL-010620/161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			executed later in the victims browser. **CVE ID : CVE-2020-13641**		
ISC					
bind					
Uncontrolled Resource Consumption	19-05-2020	5	A malicious actor who intentionally exploits this lack of effective limitation on the number of fetches performed when processing referrals can, through the use of specially crafted referrals, cause a recursing server to issue a very large number of fetches in an attempt to process the referral. This has at least two potential effects: The performance of the recursing server can potentially be degraded by the additional work required to perform these fetches, and The attacker can exploit this behavior to use the recursing server as a reflector in a reflection attack with a high amplification factor. **CVE ID : CVE-2020-8616**	https://kb.isc.org/docs/cve-2020-8616, https://security.netapp.com/advisory/ntap-20200522-0002/, https://www.synology.com/security/advisory/Synology_SA_20_12	A-ISC-BIND-010620/162
Reachable Assertion	19-05-2020	5	Using a specially-crafted message, an attacker may potentially cause a BIND server to reach an inconsistent state if the attacker knows (or successfully guesses) the name of a TSIG key used by the server. Since BIND, by	https://kb.isc.org/docs/cve-2020-8617, https://security.netapp.com/advisory/	A-ISC-BIND-010620/163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			default, configures a local session key even on servers whose configuration does not otherwise make use of it, almost all current BIND servers are vulnerable. In releases of BIND dating from March 2018 and after, an assertion check in tsig.c detects this inconsistent state and deliberately exits. Prior to the introduction of the check the server would continue operating in an inconsistent state, with potentially harmful results. **CVE ID : CVE-2020-8617**	ntap-20200522-0002/	
jenzabar					
internet_campus_solution					
Session Fixation	19-05-2020	5	Jenzabar JICS (aka Internet Campus Solution) before 9.0.1 Patch 3, 9.1 before 9.1.2 Patch 2, and 9.2 before 9.2.2 Patch 8 has session cookies that are a deterministic function of the username. There is a hard-coded password to supply a PBKDF feeding into AES to encrypt a username and base64 encode it to a client-side cookie for persistent session authentication. By knowing the key and algorithm, an attacker can select any username, encrypt it, base64 encode it, and save it in their browser with the correct	N/A	A-JEN-INTE-010620/164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			JICSLoginCookie cookie format to impersonate any real user in the JICS database without the need for authenticating (or verifying with MFA if implemented). **CVE ID : CVE-2020-8434**		
Jerryscript					
jerryscript					
Reachable Assertion	27-05-2020	5	JerryScript 2.2.0 allows attackers to cause a denial of service (assertion failure) because a property key query for a Proxy object returns unintended data. **CVE ID : CVE-2020-13622**	N/A	A-JER-JERR-010620/165
Uncontrolled Resource Consumption	27-05-2020	5	JerryScript 2.2.0 allows attackers to cause a denial of service (stack consumption) via a proxy operation. **CVE ID : CVE-2020-13623**	N/A	A-JER-JERR-010620/166
NULL Pointer Dereference	28-05-2020	5	parser/js/js-scanner.c in JerryScript 2.2.0 mishandles errors during certain out-of-memory conditions, as demonstrated by a scanner_reverse_info_list NULL pointer dereference and a scanner_scan_all assertion failure. **CVE ID : CVE-2020-13649**	N/A	A-JER-JERR-010620/167
Jquery					
jquery					
Improper Neutralization	19-05-2020	4.3	jquery prior to 1.9.0 allows Cross-site Scripting attacks	https://security.net	A-JQU-JQUE-010620/168

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input During Web Page Generation ('Cross-site Scripting')			via the load method. The load method fails to recognize and remove "<script>" HTML tags that contain a whitespace character, i.e: "</script >", which results in the enclosed script logic to be executed. **CVE ID : CVE-2020-7656**	app.com/advisory/ntap-20200528-0001/	
kaminari_project					
kaminari					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-05-2020	4.3	In Kaminari before 1.2.1, there is a vulnerability that would allow an attacker to inject arbitrary code into pages with pagination links. This has been fixed in 1.2.1. **CVE ID : CVE-2020-11082**	https://github.com/kaminari/kaminari/security/advisories/GHSA-r5jw-62xg-j433	A-KAM-KAMI-010620/169
kaoni					
ezhttptrans					
Download of Code Without Integrity Check	28-05-2020	7.5	Ezhttptrans.ocx ActiveX Control in Kaoni ezHTTPTrans 1.0.0.70 and prior versions contain a vulnerability that could allow remote attacker to download arbitrary file by setting the arguments to the activex method. This can be leveraged for code execution by rebooting the victim's PC. **CVE ID : CVE-2020-7812**	N/A	A-KAO-EZHT-010620/170
Download of Code Without	22-05-2020	7.5	Ezhttptrans.ocx ActiveX Control in Kaoni	N/A	A-KAO-EZHT-010620/171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integrity Check			ezHTTPTrans 1.0.0.70 and prior versions contain a vulnerability that could allow remote attacker to download and execute arbitrary file by setting the arguments to the activex method. This can be leveraged for code execution. **CVE ID : CVE-2020-7813**		
katacontainers					
runtime					
Improper Link Resolution Before File Access ('Link Following')	19-05-2020	2.1	An improper link resolution vulnerability affects Kata Containers versions prior to 1.11.0. Upon container teardown, a malicious guest can trick the kata-runtime into unmounting any mount point on the host and all mount points underneath it, potentiality resulting in a host DoS. **CVE ID : CVE-2020-2024**	https://github.com/kata-containers/runtime/issues/2474, https://github.com/kata-containers/runtime/pull/2475	A-KAT-RUNT-010620/172
Improper Preservation of Permissions	19-05-2020	4.6	Kata Containers before 1.11.0 on Cloud Hypervisor persists guest filesystem changes to the underlying image file on the host. A malicious guest can overwrite the image file to gain control of all subsequent guest VMs. Since Kata Containers uses the same VM image file with all VMMs, this issue may also affect QEMU and	https://github.com/kata-containers/runtime/pull/2487	A-KAT-RUNT-010620/173

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Firecracker based guests. **CVE ID : CVE-2020-2025**		
KDE					
amarok					
Uncontrolled Resource Consumption	20-05-2020	4.3	A remote user can create a specially crafted M3U file, media playlist file that when loaded by the target user, will trigger a memory leak, whereby Amarok 2.8.0 continue to waste resources over time, eventually allows attackers to cause a denial of service. **CVE ID : CVE-2020-13152**	N/A	A-KDE-AMAR-010620/174
kerberos_project					
kerberos					
Uncontrolled Search Path Element	16-05-2020	6.9	The kerberos package before 1.0.0 for Node.js allows arbitrary code execution and privilege escalation via injection of malicious DLLs through use of the kerberos_sspi LoadLibrary() method, because of a DLL path search. **CVE ID : CVE-2020-13110**	N/A	A-KER-KERB-010620/175
libexif_project					
libexif					
Out-of-bounds Read	21-05-2020	6.4	An issue was discovered in libexif before 0.6.22. Several buffer over-reads in EXIF MakerNote handling could lead to information disclosure and crashes. This is different from CVE-2020-	N/A	A-LIB-LIBE-010620/176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0093. **CVE ID : CVE-2020-13112**		
NULL Pointer Dereference	21-05-2020	5	An issue was discovered in libexif before 0.6.22. Use of uninitialized memory in EXIF Makernote handling could lead to crashes and potential use-after-free conditions. **CVE ID : CVE-2020-13113**	N/A	A-LIB-LIBE-010620/177
Uncontrolled Resource Consumption	21-05-2020	5	An issue was discovered in libexif before 0.6.22. An unrestricted size in handling Canon EXIF MakerNote data could lead to consumption of large amounts of compute time for decoding EXIF data. **CVE ID : CVE-2020-13114**	N/A	A-LIB-LIBE-010620/178
Libreoffice					
libreoffice					
Missing Encryption of Sensitive Data	18-05-2020	5	If LibreOffice has an encrypted document open and crashes, that document is auto-saved encrypted. On restart, LibreOffice offers to restore the document and prompts for the password to decrypt it. If the recovery is successful, and if the file format of the recovered document was not LibreOffice's default ODF file format, then affected versions of LibreOffice default that subsequent saves of the document are unencrypted. This may lead to a user accidentally saving	N/A	A-LIB-LIBR-010620/179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a MSOffice file format document unencrypted while believing it to be encrypted. This issue affects: LibreOffice 6-3 series versions prior to 6.3.6; 6-4 series versions prior to 6.4.3. **CVE ID : CVE-2020-12801**		
mappresspro					
mappress					
Unrestricted Upload of File with Dangerous Type	29-05-2020	6.5	The mappress-google-maps-for-wordpress plugin before 2.54.6 for WordPress does not correctly implement capability checks for AJAX functions related to creation/retrieval/deletion of PHP template files, leading to Remote Code Execution. NOTE: this issue exists because of an incomplete fix for CVE-2020-12077. **CVE ID : CVE-2020-12675**	N/A	A-MAP-MAPP-010620/180
Mariadb					
connector\/c					
N/A	20-05-2020	7.5	libmariadb/mariadb_lib.c in MariaDB Connector/C before 3.1.8 does not properly validate the content of an OK packet received from a server. NOTE: although mariadb_lib.c was originally based on code shipped for MySQL, this issue does not affect any MySQL	N/A	A-MAR-CONN-010620/181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			components supported by Oracle. **CVE ID : CVE-2020-13249**		
meinheld					
meinheld					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	22-05-2020	4.3	meinheld prior to 1.0.2 is vulnerable to HTTP Request Smuggling. HTTP pipelining issues and request smuggling attacks might be possible due to incorrect Content-Length and Transfer encoding header parsing. **CVE ID : CVE-2020-7658**	N/A	A-MEI-MEIN-010620/182
Microfocus					
enterprise_developer					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-05-2020	3.5	Cross Site scripting vulnerability on Micro Focus Enterprise Server and Enterprise developer, affecting all versions prior to version 5.0 Patch Update 8. The vulnerability could allow an attacker to trigger administrative actions when an administrator viewed malicious data left by the attacker (stored XSS) or followed a malicious link (reflected XSS). **CVE ID : CVE-2020-9524**	N/A	A-MIC-ENTE-010620/183
enterprise_server					
Improper Neutralization of Input During Web Page Generation	18-05-2020	3.5	Cross Site scripting vulnerability on Micro Focus Enterprise Server and Enterprise developer, affecting all versions prior	N/A	A-MIC-ENTE-010620/184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			to version 5.0 Patch Update 8. The vulnerability could allow an attacker to trigger administrative actions when an administrator viewed malicious data left by the attacker (stored XSS) or followed a malicious link (reflected XSS). **CVE ID : CVE-2020-9524**		
service_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-05-2020	4.3	Cross Site Scripting vulnerability in Micro Focus Service Manager product. Affecting versions 9.50, 9.51, 9.52, 9.60, 9.61, 9.62, 9.63. The vulnerability could be exploited to allow remote attackers to inject arbitrary web script or HTML. **CVE ID : CVE-2020-11845**	N/A	A-MIC-SERV-010620/185
Microsoft					
power_bi_report_server					
Improper Input Validation	21-05-2020	3.5	A spoofing vulnerability exists in Microsoft Power BI Report Server in the way it validates the content-type of uploaded attachments, aka 'Microsoft Power BI Report Server Spoofing Vulnerability'. **CVE ID : CVE-2020-1173**	N/A	A-MIC-POWE-010620/186
365_apps					
Improper Restriction of Operations within the	21-05-2020	7.5	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to	N/A	A-MIC-365_-010620/187

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-0901**		
chakracore					
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. **CVE ID : CVE-2020-1037**	N/A	A-MIC-CHAK-010620/188
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	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'. **CVE ID : CVE-2020-1065**	N/A	A-MIC-CHAK-010620/189
edge					
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. **CVE ID : CVE-2020-1037**	N/A	A-MIC-EDGE-010620/190
Incorrect Permission Assignment for	21-05-2020	5.8	An elevation of privilege vulnerability exists when Microsoft Edge does not	N/A	A-MIC-EDGE-010620/191

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Critical Resource			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-2020-1056**		
URL Redirection to Untrusted Site ('Open Redirect')	21-05-2020	4.3	A spoofing vulnerability exists when Microsoft Edge does not properly parse HTTP content, aka 'Microsoft Edge Spoofing Vulnerability'. **CVE ID : CVE-2020-1059**	N/A	A-MIC-EDGE-010620/192
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	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'. **CVE ID : CVE-2020-1065**	N/A	A-MIC-EDGE-010620/193
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists when Microsoft Edge PDF Reader improperly handles objects in memory, aka 'Microsoft Edge PDF Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1096**	N/A	A-MIC-EDGE-010620/194
Improper Privilege	21-05-2020	4.3	An elevation of privilege vulnerability exists in	N/A	A-MIC-EDGE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Microsoft Edge (Chromium-based) when the Feedback extension improperly validates input, aka 'Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1195**		010620/195
office					
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.5	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-2020-0901**	N/A	A-MIC-OFFI-010620/196
internet_explorer					
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1058, CVE-2020-1060, CVE-2020-1093. **CVE ID : CVE-2020-1035**	N/A	A-MIC-INTE-010620/197
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-	N/A	A-MIC-INTE-010620/198

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1035, CVE-2020-1060, CVE-2020-1093. **CVE ID : CVE-2020-1058**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1035, CVE-2020-1058, CVE-2020-1093. **CVE ID : CVE-2020-1060**	N/A	A-MIC-INTE-010620/199
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1092. **CVE ID : CVE-2020-1062**	N/A	A-MIC-INTE-010620/200
Improper Input Validation	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the MSHTML engine improperly validates input.An attacker could execute arbitrary code in the context of the current user, aka 'MSHTML Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1064**	N/A	A-MIC-INTE-010620/201
Improper Restriction of Operations within the	21-05-2020	7.6	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects	N/A	A-MIC-INTE-010620/202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			in memory, aka 'Internet Explorer Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1062. **CVE ID : CVE-2020-1092**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1035, CVE-2020-1058, CVE-2020-1060. **CVE ID : CVE-2020-1093**	N/A	A-MIC-INTE-010620/203
.net_framework					
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists in .NET Framework which could allow an attacker to elevate their privilege level.To exploit the vulnerability, an attacker would first have to access the local machine, and then run a malicious program.The update addresses the vulnerability by correcting how .NET Framework activates COM objects., aka '.NET Framework Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1066**	N/A	A-MIC-.NET-010620/204
visual_studio_2017					
Improper Input	21-05-2020	5	A denial of service vulnerability exists when ASP.NET Core improperly	N/A	A-MIC-VISU-010620/205

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			handles web requests, aka 'ASP.NET Core Denial of Service Vulnerability'. **CVE ID : CVE-2020-1161**		
asp.net_core					
Improper Input Validation	21-05-2020	5	A denial of service vulnerability exists when ASP.NET Core improperly handles web requests, aka 'ASP.NET Core Denial of Service Vulnerability'. **CVE ID : CVE-2020-1161**	N/A	A-MIC-ASP.-010620/206
sharepoint_server					
Unrestricted Upload of File with Dangerous Type	21-05-2020	6.5	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1024, CVE-2020-1102. **CVE ID : CVE-2020-1023**	N/A	A-MIC-SHAR-010620/207
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-05-2020	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-2020-1099, CVE-2020-1100, CVE-2020-1106. **CVE ID : CVE-2020-1101**	N/A	A-MIC-SHAR-010620/208

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	21-05-2020	6.5	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1023, CVE-2020-1024. **CVE ID : CVE-2020-1102**	N/A	A-MIC-SHAR-010620/209
Information Exposure	21-05-2020	4.3	An information disclosure vulnerability exists where certain modes of the search function in Microsoft SharePoint Server are vulnerable to cross-site search attacks (a variant of cross-site request forgery, CSRF).When users are simultaneously logged in to Microsoft SharePoint Server and visit a malicious web page, the attacker can, through standard browser functionality, induce the browser to invoke search queries as the logged in user, aka 'Microsoft SharePoint Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1103**	N/A	A-MIC-SHAR-010620/210
Unrestricted Upload of File with Dangerous Type	21-05-2020	6.5	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint	N/A	A-MIC-SHAR-010620/211

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1023, CVE-2020-1102. **CVE ID : CVE-2020-1024**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	6.5	A remote code execution vulnerability exists in Microsoft SharePoint Server when it fails to properly identify and filter unsafe ASP.Net web controls, aka 'Microsoft SharePoint Server Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1069**	N/A	A-MIC-SHAR-010620/212
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-05-2020	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-2020-1100, CVE-2020-1101, CVE-2020-1106. **CVE ID : CVE-2020-1099**	N/A	A-MIC-SHAR-010620/213
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-05-2020	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-2020-1099, CVE-2020-	N/A	A-MIC-SHAR-010620/214

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1101, CVE-2020-1106. **CVE ID : CVE-2020-1100**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-05-2020	3.5	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2020-1105, CVE-2020-1107. **CVE ID : CVE-2020-1104**	N/A	A-MIC-SHAR-010620/215
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-05-2020	3.5	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2020-1104, CVE-2020-1107. **CVE ID : CVE-2020-1105**	N/A	A-MIC-SHAR-010620/216
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-05-2020	4.3	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-2020-1099, CVE-2020-1100, CVE-2020-1101. **CVE ID : CVE-2020-1106**	N/A	A-MIC-SHAR-010620/217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-05-2020	3.5	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2020-1104, CVE-2020-1105. **CVE ID : CVE-2020-1107**	N/A	A-MIC-SHAR-010620/218
sharepoint_enterprise_server					
Unrestricted Upload of File with Dangerous Type	21-05-2020	6.5	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1024, CVE-2020-1102. **CVE ID : CVE-2020-1023**	N/A	A-MIC-SHAR-010620/219
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-05-2020	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-2020-1099, CVE-2020-1100, CVE-2020-1106. **CVE ID : CVE-2020-1101**	N/A	A-MIC-SHAR-010620/220
Unrestricted	21-05-2020	6.5	A remote code execution	N/A	A-MIC-SHAR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Upload of File with Dangerous Type			vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1023, CVE-2020-1024. **CVE ID : CVE-2020-1102**		010620/221
Information Exposure	21-05-2020	4.3	An information disclosure vulnerability exists where certain modes of the search function in Microsoft SharePoint Server are vulnerable to cross-site search attacks (a variant of cross-site request forgery, CSRF).When users are simultaneously logged in to Microsoft SharePoint Server and visit a malicious web page, the attacker can, through standard browser functionality, induce the browser to invoke search queries as the logged in user, aka 'Microsoft SharePoint Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1103**	N/A	A-MIC-SHAR-010620/222
Unrestricted Upload of File with Dangerous Type	21-05-2020	6.5	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution	N/A	A-MIC-SHAR-010620/223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. This CVE ID is unique from CVE-2020-1023, CVE-2020-1102. **CVE ID : CVE-2020-1024**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	6.5	A remote code execution vulnerability exists in Microsoft SharePoint Server when it fails to properly identify and filter unsafe ASP.Net web controls, aka 'Microsoft SharePoint Server Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1069**	N/A	A-MIC-SHAR-010620/224
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-05-2020	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-2020-1100, CVE-2020-1101, CVE-2020-1106. **CVE ID : CVE-2020-1099**	N/A	A-MIC-SHAR-010620/225
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-05-2020	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-2020-1099, CVE-2020-1101, CVE-2020-1106.	N/A	A-MIC-SHAR-010620/226

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1100		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-05-2020	3.5	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2020-1105, CVE-2020-1107. **CVE ID : CVE-2020-1104**	N/A	A-MIC-SHAR-010620/227
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-05-2020	3.5	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2020-1104, CVE-2020-1107. **CVE ID : CVE-2020-1105**	N/A	A-MIC-SHAR-010620/228
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-05-2020	4.3	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-2020-1099, CVE-2020-1100, CVE-2020-1101. **CVE ID : CVE-2020-1106**	N/A	A-MIC-SHAR-010620/229
Improper	21-05-2020	3.5	A spoofing vulnerability	N/A	A-MIC-SHAR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2020-1104, CVE-2020-1105. **CVE ID : CVE-2020-1107**		010620/230
sharepoint_foundation					
Unrestricted Upload of File with Dangerous Type	21-05-2020	6.5	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1024, CVE-2020-1102. **CVE ID : CVE-2020-1023**	N/A	A-MIC-SHAR-010620/231
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-05-2020	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-2020-1099, CVE-2020-1100, CVE-2020-1106. **CVE ID : CVE-2020-1101**	N/A	A-MIC-SHAR-010620/232
Information Exposure	21-05-2020	4.3	An information disclosure vulnerability exists where	N/A	A-MIC-SHAR-010620/233

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			certain modes of the search function in Microsoft SharePoint Server are vulnerable to cross-site search attacks (a variant of cross-site request forgery, CSRF).When users are simultaneously logged in to Microsoft SharePoint Server and visit a malicious web page, the attacker can, through standard browser functionality, induce the browser to invoke search queries as the logged in user, aka 'Microsoft SharePoint Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1103**		
Unrestricted Upload of File with Dangerous Type	21-05-2020	6.5	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1023, CVE-2020-1102. **CVE ID : CVE-2020-1024**	N/A	A-MIC-SHAR-010620/234
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	6.5	A remote code execution vulnerability exists in Microsoft SharePoint Server when it fails to properly identify and filter unsafe ASP.Net web controls, aka 'Microsoft SharePoint Server Remote Code Execution Vulnerability'.	N/A	A-MIC-SHAR-010620/235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1069		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-05-2020	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-2020-1099, CVE-2020-1101, CVE-2020-1106. **CVE ID : CVE-2020-1100**	N/A	A-MIC-SHAR-010620/236
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-05-2020	3.5	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2020-1105, CVE-2020-1107. **CVE ID : CVE-2020-1104**	N/A	A-MIC-SHAR-010620/237
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-05-2020	4.3	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-2020-1099, CVE-2020-1100, CVE-2020-1101. **CVE ID : CVE-2020-1106**	N/A	A-MIC-SHAR-010620/238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-05-2020	3.5	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'. This CVE ID is unique from CVE-2020-1104, CVE-2020-1105. **CVE ID : CVE-2020-1107**	N/A	A-MIC-SHAR-010620/239
visual_studio_code					
Improper Input Validation	21-05-2020	9.3	A remote code execution vulnerability exists in Visual Studio Code when the Python extension loads configuration files after opening a project, aka 'Visual Studio Code Python Extension Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1192. **CVE ID : CVE-2020-1171**	N/A	A-MIC-VISU-010620/240
Improper Input Validation	21-05-2020	9.3	A remote code execution vulnerability exists in Visual Studio Code when the Python extension loads workspace settings from a notebook file, aka 'Visual Studio Code Python Extension Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1171. **CVE ID : CVE-2020-1192**	N/A	A-MIC-VISU-010620/241
visual_studio_2019					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	21-05-2020	5	A denial of service vulnerability exists when ASP.NET Core improperly handles web requests, aka 'ASP.NET Core Denial of Service Vulnerability'. **CVE ID : CVE-2020-1161**	N/A	A-MIC-VISU-010620/242
dynamics_365					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-05-2020	3.5	A cross site scripting vulnerability exists when Microsoft Dynamics 365 (on-premises) does not properly sanitize a specially crafted web request to an affected Dynamics server, aka 'Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability'. **CVE ID : CVE-2020-1063**	N/A	A-MIC-DYNA-010620/243
Microweber					
microweber					
Unrestricted Upload of File with Dangerous Type	20-05-2020	7.2	Microweber 1.1.18 allows Unrestricted File Upload because admin/view:modules/load_module:users#edit-user=1 does not verify that the file extension (used with the Add Image option on the Edit User screen) corresponds to an image file. **CVE ID : CVE-2020-13241**	N/A	A-MIC-MICR-010620/244
mikrotik-router-monitoring-system_project					
mikrotik-router-monitoring-system					
Improper Neutralization of Special	16-05-2020	7.5	An issue was discovered in Mikrotik-Router-Monitoring-System through	N/A	A-MIK-MIKR-010620/245

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			2018-10-22. SQL Injection exists in check_community.php via the parameter community. **CVE ID : CVE-2020-13118**		
Misp					
misp					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-05-2020	4.3	app/View/Events/resolved_attributes.ctp in MISP before 2.4.126 has XSS in the resolved attributes view. **CVE ID : CVE-2020-13153**	N/A	A-MIS-MISP-010620/246
Monstra					
monstra					
Unrestricted Upload of File with Dangerous Type	22-05-2020	6.5	Monstra CMS 3.0.4 allows remote authenticated users to upload and execute arbitrary PHP code via admin/index.php?id=filesmanager because, for example, .php filenames are blocked but .php7 filenames are not, a related issue to CVE-2017-18048. **CVE ID : CVE-2020-13384**	N/A	A-MON-MONS-010620/247
Moodle					
moodle					
Improper Input Validation	21-05-2020	6.5	A flaw was found in Moodle versions 3.8 before 3.8.3, 3.7 before 3.7.6, 3.6 before 3.6.10, 3.5 before 3.5.12 and earlier unsupported versions. It was possible to create a SCORM package in such a way that when added to a course, it could be	http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-	A-MOO-MOOD-010620/248

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interacted with via web services in order to achieve remote code execution. **CVE ID : CVE-2020-10738**	68410, https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10738, https://moodle.org/mod/forum/discuss.php?d=403513	
Mozilla					
firefox					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	26-05-2020	6.8	A race condition when running shutdown code for Web Worker led to a use-after-free vulnerability. This resulted in a potentially exploitable crash. This vulnerability affects Firefox ESR < 68.8, Firefox < 76, and Thunderbird < 68.8.0. **CVE ID : CVE-2020-12387**	N/A	A-MOZ-FIRE-010620/249
Improper Input Validation	26-05-2020	7.5	The Firefox content processes did not sufficiently lockdown access control which could result in a sandbox escape. *Note: this issue only affects Firefox on Windows operating systems.*. This vulnerability affects Firefox ESR < 68.8 and Firefox < 76. **CVE ID : CVE-2020-12388**	N/A	A-MOZ-FIRE-010620/250
Improper Input	26-05-2020	7.5	The Firefox content processes did not	N/A	A-MOZ-FIRE-010620/251

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			sufficiently lockdown access control which could result in a sandbox escape. *Note: this issue only affects Firefox on Windows operating systems.*. This vulnerability affects Firefox ESR < 68.8 and Firefox < 76. **CVE ID : CVE-2020-12389**		
Deserialization of Untrusted Data	26-05-2020	7.5	Incorrect origin serialization of URLs with IPv6 addresses could lead to incorrect security checks. This vulnerability affects Firefox < 76. **CVE ID : CVE-2020-12390**	N/A	A-MOZ-FIRE-010620/252
Improper Input Validation	26-05-2020	5	Documents formed using data: URLs in an OBJECT element failed to inherit the CSP of the creating context. This allowed the execution of scripts that should have been blocked, albeit with a unique opaque origin. This vulnerability affects Firefox < 76. **CVE ID : CVE-2020-12391**	N/A	A-MOZ-FIRE-010620/253
Information Exposure	26-05-2020	2.1	The 'Copy as cURL' feature of Devtools' network tab did not properly escape the HTTP POST data of a request, which can be controlled by the website. If a user used the 'Copy as cURL' feature and pasted the command into a terminal, it could have resulted in the disclosure of local files. This vulnerability	N/A	A-MOZ-FIRE-010620/254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affects Firefox ESR < 68.8, Firefox < 76, and Thunderbird < 68.8.0. **CVE ID : CVE-2020-12392**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	26-05-2020	4.6	The 'Copy as cURL' feature of Devtools' network tab did not properly escape the HTTP method of a request, which can be controlled by the website. If a user used the 'Copy as cURL' feature and pasted the command into a terminal, it could have resulted in command injection and arbitrary command execution. *Note: this issue only affects Firefox on Windows operating systems.*. This vulnerability affects Firefox ESR < 68.8, Firefox < 76, and Thunderbird < 68.8.0. **CVE ID : CVE-2020-12393**	N/A	A-MOZ-FIRE-010620/255
Improper Input Validation	26-05-2020	2.1	A logic flaw in our location bar implementation could have allowed a local attacker to spoof the current location by selecting a different origin and removing focus from the input element. This vulnerability affects Firefox < 76. **CVE ID : CVE-2020-12394**	N/A	A-MOZ-FIRE-010620/256
Improper Restriction of Operations within the Bounds of a	26-05-2020	10	Mozilla developers and community members reported memory safety bugs present in Firefox 75 and Firefox ESR 68.7. Some	N/A	A-MOZ-FIRE-010620/257

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox ESR < 68.8, Firefox < 76, and Thunderbird < 68.8.0. **CVE ID : CVE-2020-12395**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	26-05-2020	7.5	Mozilla developers and community members reported memory safety bugs present in Firefox 75. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 76. **CVE ID : CVE-2020-12396**	N/A	A-MOZ-FIRE-010620/258
Information Exposure	26-05-2020	5	For native-to-JS bridging, the app requires a unique token to be passed that ensures non-app code can't call the bridging functions. That token was being used for JS-to-native also, but it isn't needed in this case, and its usage was also leaking this token. This vulnerability affects Firefox for iOS < 25. **CVE ID : CVE-2020-6830**	N/A	A-MOZ-FIRE-010620/259
Buffer Copy	26-05-2020	7.5	A buffer overflow could	N/A	A-MOZ-FIRE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			occur when parsing and validating SCTP chunks in WebRTC. This could have led to memory corruption and a potentially exploitable crash. This vulnerability affects Firefox ESR < 68.8, Firefox < 76, and Thunderbird < 68.8.0. **CVE ID : CVE-2020-6831**		010620/260
firefox_esr					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	26-05-2020	6.8	A race condition when running shutdown code for Web Worker led to a use-after-free vulnerability. This resulted in a potentially exploitable crash. This vulnerability affects Firefox ESR < 68.8, Firefox < 76, and Thunderbird < 68.8.0. **CVE ID : CVE-2020-12387**	N/A	A-MOZ-FIRE-010620/261
Improper Input Validation	26-05-2020	7.5	The Firefox content processes did not sufficiently lockdown access control which could result in a sandbox escape. *Note: this issue only affects Firefox on Windows operating systems.*. This vulnerability affects Firefox ESR < 68.8 and Firefox < 76. **CVE ID : CVE-2020-12388**	N/A	A-MOZ-FIRE-010620/262
Improper Input Validation	26-05-2020	7.5	The Firefox content processes did not sufficiently lockdown access control which could result in a sandbox escape. *Note: this issue only affects Firefox on Windows	N/A	A-MOZ-FIRE-010620/263

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating systems.*. This vulnerability affects Firefox ESR < 68.8 and Firefox < 76. **CVE ID : CVE-2020-12389**		
Information Exposure	26-05-2020	2.1	The 'Copy as cURL' feature of Devtools' network tab did not properly escape the HTTP POST data of a request, which can be controlled by the website. If a user used the 'Copy as cURL' feature and pasted the command into a terminal, it could have resulted in the disclosure of local files. This vulnerability affects Firefox ESR < 68.8, Firefox < 76, and Thunderbird < 68.8.0. **CVE ID : CVE-2020-12392**	N/A	A-MOZ-FIRE-010620/264
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	26-05-2020	4.6	The 'Copy as cURL' feature of Devtools' network tab did not properly escape the HTTP method of a request, which can be controlled by the website. If a user used the 'Copy as cURL' feature and pasted the command into a terminal, it could have resulted in command injection and arbitrary command execution. *Note: this issue only affects Firefox on Windows operating systems.*. This vulnerability affects Firefox ESR < 68.8, Firefox < 76, and Thunderbird < 68.8.0. **CVE ID : CVE-2020-12393**	N/A	A-MOZ-FIRE-010620/265

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	26-05-2020	10	Mozilla developers and community members reported memory safety bugs present in Firefox 75 and Firefox ESR 68.7. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox ESR < 68.8, Firefox < 76, and Thunderbird < 68.8.0. **CVE ID : CVE-2020-12395**	N/A	A-MOZ-FIRE-010620/266
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	26-05-2020	7.5	A buffer overflow could occur when parsing and validating SCTP chunks in WebRTC. This could have led to memory corruption and a potentially exploitable crash. This vulnerability affects Firefox ESR < 68.8, Firefox < 76, and Thunderbird < 68.8.0. **CVE ID : CVE-2020-6831**	N/A	A-MOZ-FIRE-010620/267
thunderbird					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	26-05-2020	6.8	A race condition when running shutdown code for Web Worker led to a use-after-free vulnerability. This resulted in a potentially exploitable crash. This vulnerability affects Firefox ESR < 68.8, Firefox < 76, and Thunderbird < 68.8.0. **CVE ID : CVE-2020-12387**	N/A	A-MOZ-THUN-010620/268
Information	26-05-2020	2.1	The 'Copy as cURL' feature	N/A	A-MOZ-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			of Devtools' network tab did not properly escape the HTTP POST data of a request, which can be controlled by the website. If a user used the 'Copy as cURL' feature and pasted the command into a terminal, it could have resulted in the disclosure of local files. This vulnerability affects Firefox ESR < 68.8, Firefox < 76, and Thunderbird < 68.8.0. **CVE ID : CVE-2020-12392**		THUN-010620/269
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	26-05-2020	4.6	The 'Copy as cURL' feature of Devtools' network tab did not properly escape the HTTP method of a request, which can be controlled by the website. If a user used the 'Copy as cURL' feature and pasted the command into a terminal, it could have resulted in command injection and arbitrary command execution. *Note: this issue only affects Firefox on Windows operating systems.*. This vulnerability affects Firefox ESR < 68.8, Firefox < 76, and Thunderbird < 68.8.0. **CVE ID : CVE-2020-12393**	N/A	A-MOZ-THUN-010620/270
Improper Restriction of Operations within the Bounds of a Memory Buffer	26-05-2020	10	Mozilla developers and community members reported memory safety bugs present in Firefox 75 and Firefox ESR 68.7. Some of these bugs showed	N/A	A-MOZ-THUN-010620/271

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox ESR < 68.8, Firefox < 76, and Thunderbird < 68.8.0. **CVE ID : CVE-2020-12395**		
Origin Validation Error	22-05-2020	4.3	By encoding Unicode whitespace characters within the From email header, an attacker can spoof the sender email address that Thunderbird displays. This vulnerability affects Thunderbird < 68.8.0. **CVE ID : CVE-2020-12397**	N/A	A-MOZ-THUN-010620/272
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	26-05-2020	7.5	A buffer overflow could occur when parsing and validating SCTP chunks in WebRTC. This could have led to memory corruption and a potentially exploitable crash. This vulnerability affects Firefox ESR < 68.8, Firefox < 76, and Thunderbird < 68.8.0. **CVE ID : CVE-2020-6831**	N/A	A-MOZ-THUN-010620/273
msi					
dragon_center					
Incorrect Default Permissions	18-05-2020	4.6	Weak permissions on the "%PROGRAMDATA%\MSI\ Dragon Center" folder in Dragon Center before 2.6.2003.2401, shipped with Micro-Star MSI Gaming	N/A	A-MSI-DRAG-010620/274

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			laptops, allows local authenticated users to overwrite system files and gain escalated privileges. One attack method is to change the Recommended App binary within App.json. Another attack method is to use this part of %PROGRAMDATA% for mounting an RPC Control directory. **CVE ID : CVE-2020-13149**		
Mylittletools					
mylittleadmin					
Improper Input Validation	19-05-2020	7.5	The management tool in MyLittleAdmin 3.8 allows remote attackers to execute arbitrary code because machineKey is hardcoded (the same for all customers' installations) in web.config, and can be used to send serialized ASP code. **CVE ID : CVE-2020-13166**	N/A	A-MYL-MYLI-010620/275
Naver					
whale_browser_installer					
Improper Verification of Cryptographic Signature	20-05-2020	6.4	Whale Browser Installer before 1.2.0.5 versions don't support signature verification for Flash installer. **CVE ID : CVE-2020-9753**	https://cve.naver.com/detail/cve-2020-9753	A-NAV-WHAL-010620/276
naviserver_project					
naviserver					
Improper Restriction of	16-05-2020	5	NaviServer 4.99.4 to 4.99.19 allows denial of service due	N/A	A-NAV-NAVI-010620/277

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			to the nsd/driver.c ChunkedDecode function not properly validating the length of a chunk. A remote attacker can craft a chunked-transfer request that will result in a negative value being passed to memmove via the size parameter, causing the process to crash. **CVE ID : CVE-2020-13111**		
netqmail					
netqmail					
Improper Input Validation	26-05-2020	5	qmail-verify as used in netqmail 1.06 is prone to a mail-address verification bypass vulnerability. **CVE ID : CVE-2020-3811**	https://bugs.debian.org/961060, https://www.openwall.com/lists/oss-security/2020/05/19/8	A-NET-NETQ-010620/278
Information Exposure	26-05-2020	2.1	qmail-verify as used in netqmail 1.06 is prone to an information disclosure vulnerability. A local attacker can test for the existence of files and directories anywhere in the filesystem because qmail-verify runs as root and tests for the existence of files in the attacker's home directory, without dropping its privileges first. **CVE ID : CVE-2020-3812**	https://bugs.debian.org/961060, https://www.openwall.com/lists/oss-security/2020/05/19/8	A-NET-NETQ-010620/279

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Netsweeper					
netsweeper					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-05-2020	7.5	Netsweeper through 6.4.3 allows unauthenticated remote code execution because webadmin/tools/unixlogin.php (with certain Referer headers) launches a command line with client-supplied parameters, and allows injection of shell metacharacters. **CVE ID : CVE-2020-13167**	N/A	A-NET-NETS-010620/280
nic					
knot_resolver					
Uncontrolled Resource Consumption	19-05-2020	5	Knot Resolver before 5.1.1 allows traffic amplification via a crafted DNS answer from an attacker-controlled server, aka an "NXNSAttack" issue. This is triggered by random subdomains in the NSDNAME in NS records. **CVE ID : CVE-2020-12667**	https://www.knot-resolver.cz/2020-05-19-knot-resolver-5.1.1.html	A-NIC-KNOT-010620/281
Nlnetlabs					
unbound					
Uncontrolled Recursion	19-05-2020	5	Unbound before 1.10.1 has Insufficient Control of Network Message Volume, aka an "NXNSAttack" issue. This is triggered by random subdomains in the NSDNAME in NS records. **CVE ID : CVE-2020-12662**	https://nlnetlabs.nl/downloads/unbound/CVE-2020-12662_2020-12663.txt, https://w	A-NLN-UNBO-010620/282

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ww.synology.com/security/advisory/Synology_SA_20_12	
Loop with Unreachable Exit Condition ('Infinite Loop')	19-05-2020	5	Unbound before 1.10.1 has an infinite loop via malformed DNS answers received from upstream servers. **CVE ID : CVE-2020-12663**	https://nlnetlabs.nl/downloads/unbound/CVE-2020-12662_2020-12663.txt	A-NLN-UNBO-010620/283
node-dns-sync_project					
node-dns-sync					
Improper Control of Generation of Code ('Code Injection')	28-05-2020	7.5	node-dns-sync (npm module dns-sync) through 0.2.0 allows execution of arbitrary commands . This issue may lead to remote code execution if a client of the library calls the vulnerable method with untrusted input. This has been fixed in 0.2.1. **CVE ID : CVE-2020-11079**	https://github.com/skoranga/node-dns-sync/security/advisories/GHSA-wh69-wc6q-7888	A-NOD-NODE-010620/284
ocproducts					
composr					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-05-2020	3.5	Composr 10.0.30 allows Persistent XSS via a Usergroup name under the Security configuration. **CVE ID : CVE-2020-8789**	N/A	A-OCP-COMP-010620/285
Opensuse					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
open_build_service					
Improper Privilege Management	19-05-2020	4.3	a Improper Access Control vulnerability in of Open Build Service allows remote attackers to read files of an OBS package where the sourceaccess/access is disabled This issue affects: Open Build Service versions prior to 2.10.5. **CVE ID : CVE-2020-8021**	https://bugzilla.suse.com/show_bug.cgi?id=1171649	A-OPE-OPEN-010620/286
Paidmembershipspro					
paid_memberships_pro					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-05-2020	6.5	SQL injection vulnerability in the Paid Memberships versions prior to 2.3.3 allows attacker with administrator rights to execute arbitrary SQL commands via unspecified vectors. **CVE ID : CVE-2020-5579**	N/A	A-PAI-PAID-010620/287
pcs					
dexicon_enterprise					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-05-2020	4.3	PCS DEXICON 3.4.1 allows XSS via the loginName parameter in login_action.jsp. **CVE ID : CVE-2020-6956**	N/A	A-PCS-DEXI-010620/288
Phpipam					
phpipam					
Improper Neutralization of Input During Web Page	20-05-2020	3.5	phpIPAM 1.4 contains a stored cross site scripting (XSS) vulnerability within the Edit User Instructions	N/A	A-PHP-PHPI-010620/289

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			field of the User Instructions widget. **CVE ID : CVE-2020-13225**		
pichi_project					
pichi					
Improper Certificate Validation	26-05-2020	4.3	The boost ASIO wrapper in net/asio.cpp in Pichi before 1.3.0 lacks TLS hostname verification. **CVE ID : CVE-2020-13616**	N/A	A-PIC-PICH-010620/290
pickplugins					
accordion					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-05-2020	3.5	An issue was discovered in the Accordion plugin before 2.2.9 for WordPress. The unprotected AJAX wp_ajax_accordions_ajax_import_json action allowed any authenticated user with Subscriber or higher permissions the ability to import a new accordion and inject malicious JavaScript as part of the accordion. **CVE ID : CVE-2020-13644**	N/A	A-PIC-ACCO-010620/291
pi-hole					
pi-hole					
N/A	29-05-2020	6.5	Pi-hole Web v4.3.2 (aka AdminLTE) allows Remote Code Execution by privileged dashboard users via a crafted DHCP static lease. **CVE ID : CVE-2020-8816**	http://packetstormsecurity.com/files/157861/Pi-Hole-4.3.2-DHCP-MAC-OS-Command	A-PI--PI-H-010620/292

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				- Execution .html	
Powerdns					
recursor					
Out-of-bounds Read	19-05-2020	6.5	An issue has been found in PowerDNS Recursor 4.1.0 up to and including 4.3.0. It allows an attacker (with enough privileges to change the system's hostname) to cause disclosure of uninitialized memory content via a stack-based out-of-bounds read. It only occurs on systems where gethostname() does not have '\0' termination of the returned string if the hostname is larger than the supplied buffer. (Linux systems are not affected because the buffer is always large enough. OpenBSD systems are not affected because the returned hostname always has '\0' termination.) Under some conditions, this issue can lead to the writing of one '\0' byte out-of-bounds on the stack, causing a denial of service or possibly arbitrary code execution. **CVE ID : CVE-2020-10030**	https://doc.powerdns.com/recursor/security-advisories/powerdns-advisory-2020-03.html	A-POW-RECU-010620/293
Uncontrolled Recursion	19-05-2020	5	PowerDNS Recursor from 4.1.0 up to and including 4.3.0 does not sufficiently defend against amplification attacks. An	https://doc.powerdns.com/recursor/security-	A-POW-RECU-010620/294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue in the DNS protocol has been found that allow malicious parties to use recursive DNS services to attack third party authoritative name servers. The attack uses a crafted reply by an authoritative name server to amplify the resulting traffic between the recursive and other authoritative name servers. Both types of service can suffer degraded performance as an effect. This is triggered by random subdomains in the NSDNAME in NS records. PowerDNS Recursor 4.1.16, 4.2.2 and 4.3.1 contain a mitigation to limit the impact of this DNS protocol issue. **CVE ID : CVE-2020-10995**	advisories /powerdn s-advisory-2020-01.html	
Improper Input Validation	19-05-2020	5	An issue has been found in PowerDNS Recursor 4.1.0 through 4.3.0 where records in the answer section of a NXDOMAIN response lacking an SOA were not properly validated in SyncRes::processAnswer, allowing an attacker to bypass DNSSEC validation. **CVE ID : CVE-2020-12244**	https://doc.powerdns.com/recursor/security-advisories/powerdns-advisory-2020-02.html	A-POW-RECU-010620/295
puma					
puma					
Inconsistent Interpretation	22-05-2020	5	In Puma (RubyGem) before 4.3.4 and 3.12.5, an attacker	https://github.com	A-PUM-PUMA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of HTTP Requests ('HTTP Request Smuggling')			could smuggle an HTTP response, by using an invalid transfer-encoding header. The problem has been fixed in Puma 3.12.5 and Puma 4.3.4. **CVE ID : CVE-2020-11076**	/puma/puma/security/advisories/GHSA-x7jg-6pwg-fx5h	010620/296
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	22-05-2020	5	In Puma (RubyGem) before 4.3.5 and 3.12.6, a client could smuggle a request through a proxy, causing the proxy to send a response back to another unknown client. If the proxy uses persistent connections and the client adds another request in via HTTP pipelining, the proxy may mistake it as the first request's body. Puma, however, would see it as two requests, and when processing the second request, send back a response that the proxy does not expect. If the proxy has reused the persistent connection to Puma to send another request for a different client, the second response from the first client will be sent to the second client. This is a similar but different vulnerability from CVE-2020-11076. The problem has been fixed in Puma 3.12.6 and Puma 4.3.5. **CVE ID : CVE-2020-11077**	https://github.com/puma/puma/security/advisories/GHSA-w64w-qqph-5gxm	A-PUM-PUMA-010620/297
Python					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
jw.util					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-05-2020	7.5	An exploitable vulnerability exists in the configuration-loading functionality of the jw.util package before 2.3 for Python. When loading a configuration with FromString or FromStream with YAML, one can execute arbitrary Python code, resulting in OS command execution, because safe_load is not used. **CVE ID : CVE-2020-13388**	https://security.netapp.com/advisory/ntap-20200528-0002/	A-PYT-JW.U-010620/298
Qemu					
qemu					
Out-of-bounds Read	27-05-2020	2.1	sd_wp_addr in hw/sd/sd.c in QEMU 4.2.0 uses an unvalidated address, which leads to an out-of-bounds read during sdhci_write() operations. A guest OS user can crash the QEMU process. **CVE ID : CVE-2020-13253**	http://www.openwall.com/lists/oss-security/2020/05/27/2, https://bugzilla.redhat.com/show_bug.cgi?id=1838546	A-QEM-QEMU-010620/299
Out-of-bounds Write	28-05-2020	2.1	In QEMU 4.2.0, es1370_transfer_audio in hw/audio/es1370.c does not properly validate the frame count, which allows guest OS users to trigger an out-of-bounds access during an es1370_write() operation. **CVE ID : CVE-2020-13361**	http://www.openwall.com/lists/oss-security/2020/05/28/1	A-QEM-QEMU-010620/300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	28-05-2020	2.1	In QEMU 4.2.0, megasas_lookup_frame in hw/scsi/megasas.c has an out-of-bounds read via a crafted reply_queue_head field from a guest OS user. **CVE ID : CVE-2020-13362**	http://www.openwall.com/lists/oss-security/2020/05/28/2	A-QEM-QEMU-010620/301
qore					
qore					
Improper Certificate Validation	26-05-2020	4.3	lib/QoreSocket.cpp in Qore before 0.9.4.2 lacks hostname verification for X.509 certificates. **CVE ID : CVE-2020-13615**	N/A	A-QOR-QORE-010620/302
raonwiz					
raon_k_upload					
Argument Injection or Modification	21-05-2020	7.5	In RAONWIZ K Upload v2018.0.2.51 and prior, automatic update processing without integrity check on update module(web.js) allows an attacker to modify arguments which causes downloading a random DLL and injection on it. **CVE ID : CVE-2020-7808**	https://www.boho.or.kr/krcert/secNoticeView.do?bulletin_writing_sequence=35424	A-RAO-RAON-010620/303
rconfig					
rconfig					
Unrestricted Upload of File with Dangerous Type	18-05-2020	6.5	rConfig 3.9.4 is vulnerable to remote code execution due to improper validation in the file upload functionality. vendor.crud.php accepts a file upload by checking content-type without	N/A	A-RCO-RCON-010620/304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			considering the file extension and header. Thus, an attacker can exploit this by uploading a .php file to vendor.php that contains arbitrary PHP code and changing the content-type to image/gif. **CVE ID : CVE-2020-12255**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-05-2020	3.5	rConfig 3.9.4 is vulnerable to reflected XSS. The devicemgmnt.php file improperly validates user input. An attacker can exploit this by crafting arbitrary JavaScript in the deviceId GET parameter to devicemgmnt.php. **CVE ID : CVE-2020-12256**	N/A	A-RCO-RCON-010620/305
Cross-Site Request Forgery (CSRF)	18-05-2020	6.8	rConfig 3.9.4 is vulnerable to cross-site request forgery (CSRF) because it lacks implementation of CSRF protection such as a CSRF token. An attacker can leverage this vulnerability by creating a form (add a user, delete a user, or edit a user). **CVE ID : CVE-2020-12257**	N/A	A-RCO-RCON-010620/306
Session Fixation	18-05-2020	6.4	rConfig 3.9.4 is vulnerable to session fixation because session expiry and randomization are mishandled. The application can reuse a session via PHPSESSID. Also, an attacker can exploit this vulnerability in conjunction	N/A	A-RCO-RCON-010620/307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with CVE-2020-12256 or CVE-2020-12259. **CVE ID : CVE-2020-12258**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-05-2020	3.5	rConfig 3.9.4 is vulnerable to reflected XSS. The configDevice.php file improperly validates user input. An attacker can exploit this vulnerability by crafting arbitrary JavaScript in the rid GET parameter of devicemgmnt.php. **CVE ID : CVE-2020-12259**	N/A	A-RCO-RCON-010620/308
rcos					
submitty					
URL Redirection to Untrusted Site ('Open Redirect')	16-05-2020	5.8	Submitty through 20.04.01 has an open redirect via authentication/login?old= during an invalid login attempt. **CVE ID : CVE-2020-13121**	N/A	A-RCO-SUBM-010620/309
Redhat					
resteasy					
Improper Input Validation	19-05-2020	5	A flaw was found in all resteasy 3.x.x versions prior to 3.12.0.Final and all resteasy 4.x.x versions prior to 4.6.0.Final, where an improper input validation results in returning an illegal header that integrates into the server's response. This flaw may result in an injection, which leads to unexpected behavior when the HTTP response is constructed.	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1695	A-RED-REST-010620/310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1695		
virtualization_host					
NULL Pointer Dereference	22-05-2020	5	A NULL pointer dereference flaw was found in the Linux kernel's SELinux subsystem in versions before 5.7. This flaw occurs while importing the Commercial IP Security Option (CIPSO) protocol's category bitmap into the SELinux extensible bitmap via the' ebitmap_netlbl_import' routine. While processing the CIPSO restricted bitmap tag in the 'cipso_v4_parsetag_rbm' routine, it sets the security attribute to indicate that the category bitmap is present, even if it has not been allocated. This issue leads to a NULL pointer dereference issue while importing the same category bitmap into SELinux. This flaw allows a remote network user to crash the system kernel, resulting in a denial of service. **CVE ID : CVE-2020-10711**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10711, https://www.openwall.com/lists/oss-security/2020/05/12/2	A-RED-VIRT-010620/311
openstack					
NULL Pointer Dereference	22-05-2020	5	A NULL pointer dereference flaw was found in the Linux kernel's SELinux subsystem in versions before 5.7. This flaw occurs while importing the Commercial IP Security Option (CIPSO) protocol's category bitmap into the	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10711, https://w	A-RED-OPEN-010620/312

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SELinux extensible bitmap via the' ebitmap_netlbl_import' routine. While processing the CIPSO restricted bitmap tag in the 'cipso_v4_parsetag_rbm' routine, it sets the security attribute to indicate that the category bitmap is present, even if it has not been allocated. This issue leads to a NULL pointer dereference issue while importing the same category bitmap into SELinux. This flaw allows a remote network user to crash the system kernel, resulting in a denial of service. **CVE ID : CVE-2020-10711**	ww.openwall.com/lists/oss-security/2020/05/12/2	
undertow					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	26-05-2020	6.4	A flaw was found in Undertow in versions before 2.1.1.Final, regarding the processing of invalid HTTP requests with large chunk sizes. This flaw allows an attacker to take advantage of HTTP request smuggling. **CVE ID : CVE-2020-10719**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10719	A-RED-UNDE-010620/313
3scale					
NULL Pointer Dereference	22-05-2020	5	A NULL pointer dereference flaw was found in the Linux kernel's SELinux subsystem in versions before 5.7. This flaw occurs while importing the Commercial IP Security	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-	A-RED-3SCA-010620/314

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Option (CIPSO) protocol's category bitmap into the SELinux extensible bitmap via the' ebitmap_netlbl_import' routine. While processing the CIPSO restricted bitmap tag in the 'cipso_v4_parsetag_rbm' routine, it sets the security attribute to indicate that the category bitmap is present, even if it has not been allocated. This issue leads to a NULL pointer dereference issue while importing the same category bitmap into SELinux. This flaw allows a remote network user to crash the system kernel, resulting in a denial of service. **CVE ID : CVE-2020-10711**	10711, https://www.openwall.com/lists/oss-security/2020/05/12/2	
Rockwellautomation					
eds_subsystem					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-05-2020	4.8	Products that use EDS Subsystem: Version 28.0.1 and prior (FactoryTalk Linx software (Previously called RSLinx Enterprise): Versions 6.00, 6.10, and 6.11, RSLinx Classic: Version 4.11.00 and prior, RSNetWorx software: Version 28.00.00 and prior, Studio 5000 Logix Designer software: Version 32 and prior) is vulnerable.The EDS subsystem does not provide adequate input sanitation,	N/A	A-ROC-EDS_-010620/315

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which may allow an attacker to craft specialized EDS files to inject SQL queries and manipulate the database storing the EDS files. This can lead to denial-of-service conditions. **CVE ID : CVE-2020-12034**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-05-2020	4.3	Products that use EDS Subsystem: Version 28.0.1 and prior (FactoryTalk Linx software (Previously called RSLinx Enterprise): Versions 6.00, 6.10, and 6.11, RSLinx Classic: Version 4.11.00 and prior, RSNetWorx software: Version 28.00.00 and prior, Studio 5000 Logix Designer software: Version 32 and prior) is vulnerable. A memory corruption vulnerability exists in the algorithm that matches square brackets in the EDS subsystem. This may allow an attacker to craft specialized EDS files to crash the EDSParser COM object, leading to denial-of-service conditions. **CVE ID : CVE-2020-12038**	N/A	A-ROC-EDS_-010620/316
rsnetworx					
Improper Neutralization of Special Elements used in an SQL Command ('SQL	20-05-2020	4.8	Products that use EDS Subsystem: Version 28.0.1 and prior (FactoryTalk Linx software (Previously called RSLinx Enterprise): Versions 6.00, 6.10, and 6.11, RSLinx Classic:	N/A	A-ROC-RSNE-010620/317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			Version 4.11.00 and prior, RSNetWorx software: Version 28.00.00 and prior, Studio 5000 Logix Designer software: Version 32 and prior) is vulnerable.The EDS subsystem does not provide adequate input sanitation, which may allow an attacker to craft specialized EDS files to inject SQL queries and manipulate the database storing the EDS files. This can lead to denial-of-service conditions. **CVE ID : CVE-2020-12034**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-05-2020	4.3	Products that use EDS Subsystem: Version 28.0.1 and prior (FactoryTalk Linx software (Previously called RSLinx Enterprise): Versions 6.00, 6.10, and 6.11, RSLinx Classic: Version 4.11.00 and prior, RSNetWorx software: Version 28.00.00 and prior, Studio 5000 Logix Designer software: Version 32 and prior) is vulnerable. A memory corruption vulnerability exists in the algorithm that matches square brackets in the EDS subsystem. This may allow an attacker to craft specialized EDS files to crash the EDSParser COM object, leading to denial-of-service conditions. **CVE ID : CVE-2020-12038**	N/A	A-ROC-RSNE-010620/318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
studio_5000_logix_designer					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-05-2020	4.8	Products that use EDS Subsystem: Version 28.0.1 and prior (FactoryTalk Linx software (Previously called RSLinx Enterprise): Versions 6.00, 6.10, and 6.11, RSLinx Classic: Version 4.11.00 and prior, RSNetWorx software: Version 28.00.00 and prior, Studio 5000 Logix Designer software: Version 32 and prior) is vulnerable.The EDS subsystem does not provide adequate input sanitation, which may allow an attacker to craft specialized EDS files to inject SQL queries and manipulate the database storing the EDS files. This can lead to denial-of-service conditions. **CVE ID : CVE-2020-12034**	N/A	A-ROC-STUD-010620/319
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-05-2020	4.3	Products that use EDS Subsystem: Version 28.0.1 and prior (FactoryTalk Linx software (Previously called RSLinx Enterprise): Versions 6.00, 6.10, and 6.11, RSLinx Classic: Version 4.11.00 and prior, RSNetWorx software: Version 28.00.00 and prior, Studio 5000 Logix Designer software: Version 32 and prior) is vulnerable. A memory corruption vulnerability exists in the algorithm that matches	N/A	A-ROC-STUD-010620/320

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			square brackets in the EDS subsystem. This may allow an attacker to craft specialized EDS files to crash the EDSParser COM object, leading to denial-of-service conditions. **CVE ID : CVE-2020-12038**		
rslinx_enterprise					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-05-2020	4.8	Products that use EDS Subsystem: Version 28.0.1 and prior (FactoryTalk Linx software (Previously called RSLinx Enterprise): Versions 6.00, 6.10, and 6.11, RSLinx Classic: Version 4.11.00 and prior, RSNetWorx software: Version 28.00.00 and prior, Studio 5000 Logix Designer software: Version 32 and prior) is vulnerable.The EDS subsystem does not provide adequate input sanitation, which may allow an attacker to craft specialized EDS files to inject SQL queries and manipulate the database storing the EDS files. This can lead to denial-of-service conditions. **CVE ID : CVE-2020-12034**	N/A	A-ROC-RSLI-010620/321
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-05-2020	4.3	Products that use EDS Subsystem: Version 28.0.1 and prior (FactoryTalk Linx software (Previously called RSLinx Enterprise): Versions 6.00, 6.10, and 6.11, RSLinx Classic: Version 4.11.00 and prior,	N/A	A-ROC-RSLI-010620/322

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			RSNetWorx software: Version 28.00.00 and prior, Studio 5000 Logix Designer software: Version 32 and prior) is vulnerable. A memory corruption vulnerability exists in the algorithm that matches square brackets in the EDS subsystem. This may allow an attacker to craft specialized EDS files to crash the EDSParser COM object, leading to denial-of-service conditions. **CVE ID : CVE-2020-12038**		
rslinx					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-05-2020	4.8	Products that use EDS Subsystem: Version 28.0.1 and prior (FactoryTalk Linx software (Previously called RSLinx Enterprise): Versions 6.00, 6.10, and 6.11, RSLinx Classic: Version 4.11.00 and prior, RSNetWorx software: Version 28.00.00 and prior, Studio 5000 Logix Designer software: Version 32 and prior) is vulnerable.The EDS subsystem does not provide adequate input sanitation, which may allow an attacker to craft specialized EDS files to inject SQL queries and manipulate the database storing the EDS files. This can lead to denial-of-service conditions. **CVE ID : CVE-2020-12034**	N/A	A-ROC-RSLI-010620/323

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-05-2020	4.3	Products that use EDS Subsystem: Version 28.0.1 and prior (FactoryTalk Linx software (Previously called RSLinx Enterprise): Versions 6.00, 6.10, and 6.11, RSLinx Classic: Version 4.11.00 and prior, RSNetWorx software: Version 28.00.00 and prior, Studio 5000 Logix Designer software: Version 32 and prior) is vulnerable. A memory corruption vulnerability exists in the algorithm that matches square brackets in the EDS subsystem. This may allow an attacker to craft specialized EDS files to crash the EDSParser COM object, leading to denial-of-service conditions. **CVE ID : CVE-2020-12038**	N/A	A-ROC-RSLI-010620/324
Schedmd					
slurm					
N/A	21-05-2020	5.1	Slurm 19.05.x before 19.05.7 and 20.02.x before 20.02.3, in the rare case where Message Aggregation is enabled, allows Authentication Bypass via an Alternate Path or Channel. A race condition allows a user to launch a process as an arbitrary user. **CVE ID : CVE-2020-12693**	https://lists.schedmd.com/pipermail/slurm-announce/2020/000036.html, https://www.schedmd.com/news.php?id=236	A-SCH-SLUR-010620/325

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
seta					
morita_shogi_64					
Out-of-bounds Write	16-05-2020	7.5	Morita Shogi 64 through 2020-05-02 for Nintendo 64 devices allows remote attackers to execute arbitrary code via crafted packet data to the built-in modem because 0x800b3e94 (aka the IF subcommand to top-level command 7) has a stack-based buffer overflow. **CVE ID : CVE-2020-13109**	N/A	A-SET-MORI-010620/326
signal					
signal					
Information Exposure	20-05-2020	5	Signal Private Messenger Android v4.59.0 and up and iOS v3.8.1.5 and up allows a remote non-contact to ring a victim's Signal phone and disclose currently used DNS server due to ICE Candidate handling before call is answered or declined. **CVE ID : CVE-2020-5753**	N/A	A-SIG-SIGN-010620/327
signal_private_messenger					
Information Exposure	20-05-2020	5	Signal Private Messenger Android v4.59.0 and up and iOS v3.8.1.5 and up allows a remote non-contact to ring a victim's Signal phone and disclose currently used DNS server due to ICE Candidate handling before call is answered or declined. **CVE ID : CVE-2020-5753**	N/A	A-SIG-SIGN-010620/328

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
siteorigin					
page_builder					
Cross-Site Request Forgery (CSRF)	28-05-2020	6.8	An issue was discovered in the SiteOrigin Page Builder plugin before 2.10.16 for WordPress. The action_builder_content function did not do any nonce verification, allowing for requests to be forged on behalf of an administrator. The panels_data $_POST variable allows for malicious JavaScript to be executed in the victim's browser. **CVE ID : CVE-2020-13642**	N/A	A-SIT-PAGE-010620/329
Cross-Site Request Forgery (CSRF)	28-05-2020	6.8	An issue was discovered in the SiteOrigin Page Builder plugin before 2.10.16 for WordPress. The live editor feature did not do any nonce verification, allowing for requests to be forged on behalf of an administrator. The live_editor_panels_data $_POST variable allows for malicious JavaScript to be executed in the victim's browser. **CVE ID : CVE-2020-13643**	N/A	A-SIT-PAGE-010620/330
Smartbear					
readyapi					
Improper Neutralization of Special Elements in Output Used by a Downstream	20-05-2020	7.5	An issue was discovered in SmartBear ReadyAPI SoapUI Pro 3.2.5. Due to unsafe use of an Java RMI based protocol in an unsafe configuration, an attacker	N/A	A-SMA-READ-010620/331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Component ('Injection')			can inject malicious serialized objects into the communication, resulting in remote code execution in the context of a client-side Network Licensing Protocol component. **CVE ID : CVE-2020-12835**		
Sourcefabric					
newscoop					
Unrestricted Upload of File with Dangerous Type	19-05-2020	4.6	Because of Unrestricted Upload of a File with a Dangerous Type, Sourcefabric Newscoop 4.4.7 allows an authenticated user to execute arbitrary PHP code (and sometimes terminal commands) on a server by making an avatar update and then visiting the avatar file under the /images/ path. **CVE ID : CVE-2020-11807**	N/A	A-SOU-NEWS-010620/332
splashtop					
software_updater					
Uncontrolled Search Path Element	21-05-2020	6.3	A Windows privilege change issue was discovered in Splashtop Software Updater before 1.5.6.16. Insecure permissions on the configuration file and named pipe allow for local privilege escalation to NT AUTHORITY/SYSTEM, by forcing a permission change to any Splashtop files and directories, with resultant	N/A	A-SPL-SOFT-010620/333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			DLL hijacking. This product is bundled with Splashtop Streamer (before 3.3.8.0) and Splashtop Business (before 3.3.8.0). **CVE ID : CVE-2020-12431**		
business					
Uncontrolled Search Path Element	21-05-2020	6.3	A Windows privilege change issue was discovered in Splashtop Software Updater before 1.5.6.16. Insecure permissions on the configuration file and named pipe allow for local privilege escalation to NT AUTHORITY/SYSTEM, by forcing a permission change to any Splashtop files and directories, with resultant DLL hijacking. This product is bundled with Splashtop Streamer (before 3.3.8.0) and Splashtop Business (before 3.3.8.0). **CVE ID : CVE-2020-12431**	N/A	A-SPL-BUSI-010620/334
streamer					
Uncontrolled Search Path Element	21-05-2020	6.3	A Windows privilege change issue was discovered in Splashtop Software Updater before 1.5.6.16. Insecure permissions on the configuration file and named pipe allow for local privilege escalation to NT AUTHORITY/SYSTEM, by forcing a permission change to any Splashtop files and	N/A	A-SPL-STRE-010620/335

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			directories, with resultant DLL hijacking. This product is bundled with Splashtop Streamer (before 3.3.8.0) and Splashtop Business (before 3.3.8.0). **CVE ID : CVE-2020-12431**		
Sqlite					
sqlite					
Integer Overflow or Wraparound	24-05-2020	5	SQLite through 3.32.0 has an integer overflow in sqlite3_str_vappendf in printf.c. **CVE ID : CVE-2020-13434**	https://security.netapp.com/advisory/ntap-20200528-0004/	A-SQL-SQLI-010620/336
Improper Initialization	24-05-2020	5	SQLite through 3.32.0 has a segmentation fault in sqlite3ExprCodeTarget in expr.c. **CVE ID : CVE-2020-13435**	https://security.netapp.com/advisory/ntap-20200528-0004/	A-SQL-SQLI-010620/337
Use After Free	27-05-2020	7.5	ext/fts3/fts3.c in SQLite before 3.32.0 has a use-after-free in fts3EvalNextRow, related to the snippet feature. **CVE ID : CVE-2020-13630**	N/A	A-SQL-SQLI-010620/338
N/A	27-05-2020	5	SQLite before 3.32.0 allows a virtual table to be renamed to the name of one of its shadow tables, related to alter.c and build.c. **CVE ID : CVE-2020-13631**	N/A	A-SQL-SQLI-010620/339
NULL Pointer Dereference	27-05-2020	5	ext/fts3/fts3_snippet.c in SQLite before 3.32.0 has a NULL pointer dereference	N/A	A-SQL-SQLI-010620/340

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via a crafted matchinfo() query. **CVE ID : CVE-2020-13632**		
swhouse					
c-cure_9000					
Cleartext Storage of Sensitive Information	21-05-2020	4	During installation or upgrade to Software House C•CURE 9000 v2.70 and American Dynamics victor Video Management System v5.2, the credentials of the user used to perform the installation or upgrade are logged in a file. The install log file persists after the installation. **CVE ID : CVE-2020-9045**	https://www.johnsoncontrols.com/cyber-solutions/security-advisories	A-SWH-C-CU-010620/341
Sympa					
sympa					
Improper Privilege Management	27-05-2020	7.2	Sympa before 6.2.56 allows privilege escalation. **CVE ID : CVE-2020-10936**	N/A	A-SYM-SYMP-010620/342
teradici					
pcoip_graphics_agent					
Improper Privilege Management	28-05-2020	4.6	Initialization of the pcoip_credential_provider in Teradici PCoIP Standard Agent for Windows and PCoIP Graphics Agent for Windows versions 19.11.1 and earlier creates an insecure named pipe, which allows an attacker to intercept sensitive information or possibly elevate privileges via pre-installing an application	https://advisory.teradici.com/security-advisories/55/	A-TER-PCOI-010620/343

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which acquires that named pipe. **CVE ID : CVE-2020-13173**		
pcoip_standard_agent					
Improper Privilege Management	28-05-2020	4.6	Initialization of the pcoip_credential_provider in Teradici PCoIP Standard Agent for Windows and PCoIP Graphics Agent for Windows versions 19.11.1 and earlier creates an insecure named pipe, which allows an attacker to intercept sensitive information or possibly elevate privileges via pre-installing an application which acquires that named pipe. **CVE ID : CVE-2020-13173**	https://advisory.teradici.com/security-advisories/55/	A-TER-PCOI-010620/344
Tibco					
jasperreports_library					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-05-2020	6.8	The report generator component of TIBCO Software Inc.'s TIBCO JasperReports Library, TIBCO JasperReports Library for ActiveMatrix BPM, TIBCO JasperReports Server, TIBCO JasperReports Server for AWS Marketplace, and TIBCO JasperReports Server for ActiveMatrix BPM contains a vulnerability that theoretically allows an attacker to exploit HTML injection to gain full control of a web interface	http://www.tibco.com/services/support/advisories	A-TIB-JASP-010620/345

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			containing the output of the report generator component with the privileges of any user that views the affected report(s). The attacker can theoretically exploit this vulnerability when other users view a maliciously generated report, where those reports use Fusion Charts and a data source with contents controlled by the attacker. Affected releases are TIBCO Software Inc.'s TIBCO JasperReports Library: versions 7.1.1 and below, versions 7.2.0 and 7.2.1, version 7.3.0, version 7.5.0, TIBCO JasperReports Library for ActiveMatrix BPM: versions 7.1.1 and below, TIBCO JasperReports Server: versions 7.1.1 and below, version 7.2.0, version 7.5.0, TIBCO JasperReports Server for AWS Marketplace: versions 7.5.0 and below, and TIBCO JasperReports Server for ActiveMatrix BPM: versions 7.1.1 and below. **CVE ID : CVE-2020-9410**		
jasperreports_server					
Incorrect Default Permissions	20-05-2020	10	The administrative UI component of TIBCO Software Inc.'s TIBCO JasperReports Server, TIBCO JasperReports Server	http://www.tibco.com/services/support/advis	A-TIB-JASP-010620/346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for AWS Marketplace, and TIBCO JasperReports Server for ActiveMatrix BPM contains a vulnerability that theoretically allows an unauthenticated attacker to obtain the permissions of a JasperReports Server "superuser" for the affected systems. The attacker can theoretically exploit the vulnerability consistently, remotely, and without authenticating. Affected releases are TIBCO Software Inc.'s TIBCO JasperReports Server: versions 7.1.1 and below, TIBCO JasperReports Server for AWS Marketplace: versions 7.1.1 and below, and TIBCO JasperReports Server for ActiveMatrix BPM: versions 7.1.1 and below. **CVE ID : CVE-2020-9409**	ories	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-05-2020	6.8	The report generator component of TIBCO Software Inc.'s TIBCO JasperReports Library, TIBCO JasperReports Library for ActiveMatrix BPM, TIBCO JasperReports Server, TIBCO JasperReports Server for AWS Marketplace, and TIBCO JasperReports Server for ActiveMatrix BPM contains a vulnerability that theoretically allows an attacker to exploit HTML	http://www.tibco.com/services/support/advisories	A-TIB-JASP-010620/347

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			injection to gain full control of a web interface containing the output of the report generator component with the privileges of any user that views the affected report(s). The attacker can theoretically exploit this vulnerability when other users view a maliciously generated report, where those reports use Fusion Charts and a data source with contents controlled by the attacker. Affected releases are TIBCO Software Inc.'s TIBCO JasperReports Library: versions 7.1.1 and below, versions 7.2.0 and 7.2.1, version 7.3.0, version 7.5.0, TIBCO JasperReports Library for ActiveMatrix BPM: versions 7.1.1 and below, TIBCO JasperReports Server: versions 7.1.1 and below, version 7.2.0, version 7.5.0, TIBCO JasperReports Server for AWS Marketplace: versions 7.5.0 and below, and TIBCO JasperReports Server for ActiveMatrix BPM: versions 7.1.1 and below. **CVE ID : CVE-2020-9410**		
tracetogether					
tracetogether					
N/A	18-05-2020	7.5	OpenTrace, as used in COVIDSafe through v1.0.17,	N/A	A-TRA-TRAC-010620/348

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			TraceTogether, ABTraceTogether, and other applications on iOS and Android, allows remote attackers to conduct long-term re-identification attacks and possibly have unspecified other impact, because of how Bluetooth is used. **CVE ID : CVE-2020-12856**		
Trendmicro					
interscan_web_security_virtual_appliance					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-05-2020	4.3	A cross-site scripting vulnerability (XSS) in Trend Micro InterScan Web Security Virtual Appliance 6.5 may allow a remote attacker to tamper with the web interface of affected installations. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. **CVE ID : CVE-2020-8603**	N/A	A-TRE-INTE-010620/349
Information Exposure	27-05-2020	5	A vulnerability in Trend Micro InterScan Web Security Virtual Appliance 6.5 may allow remote attackers to disclose sensitive informatoin on affected installations. **CVE ID : CVE-2020-8604**	N/A	A-TRE-INTE-010620/350
Improper Neutralization of Special Elements used	27-05-2020	6.5	A vulnerability in Trend Micro InterScan Web Security Virtual Appliance 6.5 may allow remote	N/A	A-TRE-INTE-010620/351

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
in an OS Command ('OS Command Injection')			attackers to execute arbitrary code on affected installations. Authentication is required to exploit this vulnerability. **CVE ID : CVE-2020-8605**		
Improper Authentication	27-05-2020	7.5	A vulnerability in Trend Micro InterScan Web Security Virtual Appliance 6.5 may allow remote attackers to bypass authentication on affected installations of Trend Micro InterScan Web Security Virtual Appliance. **CVE ID : CVE-2020-8606**	N/A	A-TRE-INTE-010620/352
tyco					
victor_video_management_system					
Cleartext Storage of Sensitive Information	21-05-2020	4	During installation or upgrade to Software House C•CURE 9000 v2.70 and American Dynamics victor Video Management System v5.2, the credentials of the user used to perform the installation or upgrade are logged in a file. The install log file persists after the installation. **CVE ID : CVE-2020-9045**	https://www.johnsoncontrols.com/cyber-solutions/security-advisories	A-TYC-VICT-010620/353
uaelementor					
ultimate_addons_for_elementor					
Incorrect Permission Assignment for Critical Resource	17-05-2020	6.4	An issue was discovered in the "Ultimate Addons for Elementor" plugin before 1.24.2 for WordPress, as exploited in the wild in May 2020 in conjunction with	N/A	A-UAE-ULTI-010620/354

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-13126. Unauthenticated attackers can create users with the Subscriber role even if registration is disabled. **CVE ID : CVE-2020-13125**		
Unisys					
algol_compiler					
Improper Input Validation	21-05-2020	5.9	Unisys ALGOL Compiler 58.1 before 58.1a.15, 59.1 before 59.1a.9, and 60.0 before 60.0a.5 can emit invalid code sequences under rare circumstances related to syntax. The resulting code could, for example, trigger a system fault or adversely affect confidentiality, integrity, and availability. **CVE ID : CVE-2020-12647**	https://public.support.unisys.com/common/public/vulnerability/NVD_Detail_Rpt.aspx?ID=55	A-UNI-ALGO-010620/355
verbb					
image_resizer					
Cross-Site Request Forgery (CSRF)	25-05-2020	6.8	An issue was discovered in the Image Resizer plugin before 2.0.9 for Craft CMS. There are CSRF issues with the log-clear controller action. **CVE ID : CVE-2020-13458**	N/A	A-VER-IMAG-010620/356
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-05-2020	3.5	An issue was discovered in the Image Resizer plugin before 2.0.9 for Craft CMS. There is stored XSS in the Bulk Resize action. **CVE ID : CVE-2020-13459**	N/A	A-VER-IMAG-010620/357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
knock_knock					
Incorrect Comparison	25-05-2020	6.4	The Knock Knock plugin before 1.2.8 for Craft CMS allows IP Whitelist bypass via an X-Forwarded-For HTTP header. **CVE ID : CVE-2020-13485**	N/A	A-VER-KNOC-010620/358
URL Redirection to Untrusted Site ('Open Redirect')	25-05-2020	5.8	The Knock Knock plugin before 1.2.8 for Craft CMS allows malicious redirection. **CVE ID : CVE-2020-13486**	N/A	A-VER-KNOC-010620/359
Vmware					
vcloud_director					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-05-2020	6.5	VMware Cloud Director 10.0.x before 10.0.0.2, 9.7.0.x before 9.7.0.5, 9.5.0.x before 9.5.0.6, and 9.1.0.x before 9.1.0.4 do not properly handle input leading to a code injection vulnerability. An authenticated actor may be able to send malicious traffic to VMware Cloud Director which may lead to arbitrary remote code execution. This vulnerability can be exploited through the HTML5- and Flex-based UIs, the API Explorer interface and API access. **CVE ID : CVE-2020-3956**	N/A	A-VMW-VCLO-010620/360
Wireshark					
wireshark					
Uncontrolled Resource	19-05-2020	5	In Wireshark 3.2.0 to 3.2.3, 3.0.0 to 3.0.10, and 2.6.0 to	N/A	A-WIR-WIRE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Consumption			2.6.16, the NFS dissector could crash. This was addressed in epan/dissectors/packet-nfs.c by preventing excessive recursion, such as for a cycle in the directory graph on a filesystem. **CVE ID : CVE-2020-13164**		010620/361
Wso2					
api_manager					
Server-Side Request Forgery (SSRF)	20-05-2020	7.5	WSO2 API Manager 3.0.0 does not properly restrict outbound network access from a Publisher node, opening up the possibility of SSRF to this node's entire intranet. **CVE ID : CVE-2020-13226**	N/A	A-WSO-API_-010620/362
Xcloner					
xcloner					
Information Exposure	23-05-2020	4	The XCloner component before 3.5.4 for Joomla! allows Authenticated Local File Disclosure. **CVE ID : CVE-2020-13424**	N/A	A-XCL-XCLO-010620/363
youhua					
windows_master					
Improper Input Validation	29-05-2020	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not	N/A	A-YOU-WIND-010620/364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validating input values from IOCtl 0xF1002558 **CVE ID : CVE-2020-13634**		
Zohocorp					
manageengine_servicedesk_plus					
Insufficiently Protected Credentials	18-05-2020	4	Zoho ManageEngine Service Plus before 11.1 build 11112 allows low-privilege authenticated users to discover the File Protection password via a getFileProtectionSettings call to AjaxServlet. **CVE ID : CVE-2020-13154**	N/A	A-ZOH-MANA-010620/365
Operating System					
Apple					
mac_os					
Improper Privilege Management	22-05-2020	7.5	An Elevation of Privilege issue was discovered in Aviatrix VPN Client before 2.10.7, because of an incomplete fix for CVE-2020-7224. This affects Linux, macOS, and Windows installations for certain OpenSSL parameters. **CVE ID : CVE-2020-13417**	N/A	O-APP-MAC_-010620/366
mac_os_x					
Improper Privilege Management	21-05-2020	6.8	Inappropriate implementation in installer in Google Chrome on OS X prior to 83.0.4103.61 allowed a local attacker to perform privilege escalation via a crafted file. **CVE ID : CVE-2020-6477**	N/A	O-APP-MAC_-010620/367

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bosch					
recording_station_firmware					
Exposure of Resource to Wrong Sphere	27-05-2020	7.2	Improper Access Control in the Kiosk Mode functionality of Bosch Recording Station allows a local unauthenticated attacker to escape from the Kiosk Mode and access the underlying operating system. **CVE ID : CVE-2020-6774**	N/A	O-BOS-RECO-010620/368
Canonical					
ubuntu_linux					
Integer Overflow or Wraparound	19-05-2020	4.6	A vulnerability was found in DPDK versions 18.05 and above. A missing check for an integer overflow in vhost_user_set_log_base() could result in a smaller memory map than requested, possibly allowing memory corruption. **CVE ID : CVE-2020-10722**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10722	O-CAN-UBUN-010620/369
Integer Overflow or Wraparound	19-05-2020	4.6	A memory corruption issue was found in DPDK versions 17.05 and above. This flaw is caused by an integer truncation on the index of a payload. Under certain circumstances, the index (a UInt) is copied and truncated into a uint16, which can lead to out of bound indexing and possible memory corruption.	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10723	O-CAN-UBUN-010620/370

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-10723		
Integer Overflow or Wraparound	19-05-2020	2.1	A vulnerability was found in DPDK versions 18.11 and above. The vhost-crypto library code is missing validations for user-supplied values, potentially allowing an information leak through an out-of-bounds memory read. **CVE ID : CVE-2020-10724**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10724	O-CAN-UBUN-010620/371
Debian					
debian_linux					
Integer Overflow or Wraparound	24-05-2020	5	SQLite through 3.32.0 has an integer overflow in sqlite3_str_vappendf in printf.c. **CVE ID : CVE-2020-13434**	https://security.netapp.com/advisory/ntap-20200528-0004/	O-DEB-DEBI-010620/372
Improper Input Validation	26-05-2020	5	qmail-verify as used in netqmail 1.06 is prone to a mail-address verification bypass vulnerability. **CVE ID : CVE-2020-3811**	https://bugs.debian.org/961060, https://www.openwall.com/lists/oss-security/2020/05/19/8	O-DEB-DEBI-010620/373
Information Exposure	26-05-2020	2.1	qmail-verify as used in netqmail 1.06 is prone to an information disclosure vulnerability. A local attacker can test for the existence of files and directories anywhere in the filesystem because qmail-	https://bugs.debian.org/961060, https://www.openwall.com/lists/oss-	O-DEB-DEBI-010620/374

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			verify runs as root and tests for the existence of files in the attacker's home directory, without dropping its privileges first. **CVE ID : CVE-2020-3812**	security/2020/05/19/8	
Uncontrolled Resource Consumption	19-05-2020	5	A malicious actor who intentionally exploits this lack of effective limitation on the number of fetches performed when processing referrals can, through the use of specially crafted referrals, cause a recursing server to issue a very large number of fetches in an attempt to process the referral. This has at least two potential effects: The performance of the recursing server can potentially be degraded by the additional work required to perform these fetches, and The attacker can exploit this behavior to use the recursing server as a reflector in a reflection attack with a high amplification factor. **CVE ID : CVE-2020-8616**	https://kb.isc.org/docs/cve-2020-8616, https://security.netapp.com/advisory/ntap-20200522-0002/, https://www.synology.com/security/advisory/Synology_SA_20_12	O-DEB-DEBI-010620/375
Reachable Assertion	19-05-2020	5	Using a specially-crafted message, an attacker may potentially cause a BIND server to reach an inconsistent state if the attacker knows (or successfully guesses) the name of a TSIG key used by the server. Since BIND, by	https://kb.isc.org/docs/cve-2020-8617, https://security.netapp.com/advisory/	O-DEB-DEBI-010620/376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			default, configures a local session key even on servers whose configuration does not otherwise make use of it, almost all current BIND servers are vulnerable. In releases of BIND dating from March 2018 and after, an assertion check in tsig.c detects this inconsistent state and deliberately exits. Prior to the introduction of the check the server would continue operating in an inconsistent state, with potentially harmful results. **CVE ID : CVE-2020-8617**	ntap-20200522-0002/	
Dell					
dock_wd15_firmware					
Uncontrolled Search Path Element	28-05-2020	2.6	Dell Dock Firmware Update Utilities for Dell Client Consumer and Commercial docking stations contain an Arbitrary File Overwrite vulnerability. The vulnerability is limited to the Dell Dock Firmware Update Utilities during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect	N/A	O-DEL-DOCK-010620/377

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the actual binary payload that the update utility delivers. **CVE ID : CVE-2020-5357**		
dock_wd19_firmware					
Uncontrolled Search Path Element	28-05-2020	2.6	Dell Dock Firmware Update Utilities for Dell Client Consumer and Commercial docking stations contain an Arbitrary File Overwrite vulnerability. The vulnerability is limited to the Dell Dock Firmware Update Utilities during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. **CVE ID : CVE-2020-5357**	N/A	O-DEL-DOCK-010620/378
thunderbolt_dock_tb16_firmware					
Uncontrolled Search Path Element	28-05-2020	2.6	Dell Dock Firmware Update Utilities for Dell Client Consumer and Commercial docking stations contain an Arbitrary File Overwrite vulnerability. The vulnerability is limited to the Dell Dock Firmware	N/A	O-DEL-THUN-010620/379

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Update Utilities during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. **CVE ID : CVE-2020-5357**		
precision_dual_usb-c_thunderbolt_dock_-_tb18dc_firmware					
Uncontrolled Search Path Element	28-05-2020	2.6	Dell Dock Firmware Update Utilities for Dell Client Consumer and Commercial docking stations contain an Arbitrary File Overwrite vulnerability. The vulnerability is limited to the Dell Dock Firmware Update Utilities during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload	N/A	O-DEL-PREC-010620/380

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that the update utility delivers. **CVE ID : CVE-2020-5357**		
D-link					
dsp-w215_firmware					
Information Exposure	18-05-2020	3.3	D-Link DSP-W215 1.26b03 devices allow information disclosure by intercepting messages on the local network, as demonstrated by a Squid Proxy. **CVE ID : CVE-2020-13135**	N/A	O-D-L-DSP--010620/381
Information Exposure	18-05-2020	5	D-Link DSP-W215 1.26b03 devices send an obfuscated hash that can be retrieved and understood by a network sniffer. **CVE ID : CVE-2020-13136**	N/A	O-D-L-DSP--010620/382
Epson					
eb-1470ui_firmware					
Information Exposure	22-05-2020	6.4	An exploitable authentication bypass vulnerability exists in the ESPON Web Control functionality of Epson EB-1470Ui MAIN: 98009273ESWWV107 MAIN2: 8X7325WWV303. A specially crafted series of HTTP requests can cause authentication bypass resulting in information disclosure. An attacker can send an HTTP request to trigger this vulnerability. **CVE ID : CVE-2020-6091**	N/A	O-EPS-EB-1-010620/383
Google					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
chrome_os					
Improper Input Validation	21-05-2020	4.3	Insufficient data validation in media router in Google Chrome prior to 83.0.4103.61 allowed a remote attacker who had compromised the renderer process to bypass navigation restrictions via a crafted HTML page. **CVE ID : CVE-2020-6485**	N/A	O-GOO-CHRO-010620/384
hpe					
nimbleos					
Improper Input Validation	19-05-2020	6.5	Potential remote code execution security vulnerabilities have been identified with HPE Nimble Storage systems that could be exploited by an attacker to gain elevated privileges on the array. The following NimbleOS versions, and all subsequent releases, contain a software fix for this vulnerability: 3.9.3.0 4.5.6.0 5.0.9.0 5.1.4.100 **CVE ID : CVE-2020-7138**	N/A	O-HPE-NIMB-010620/385
Information Exposure	19-05-2020	5.5	Potential remote access security vulnerabilities have been identified with HPE Nimble Storage systems that could be exploited by an attacker to access and modify sensitive information on the system. The following NimbleOS versions, and all subsequent releases, contain a software fix for this vulnerability:	N/A	O-HPE-NIMB-010620/386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.9.3.0 4.5.6.0 5.0.9.0 5.1.4.100 **CVE ID : CVE-2020-7139**		
superdome_flex_server_firmware					
Improper Input Validation	19-05-2020	4.6	A validation issue in HPE Superdome Flex's RMC component may allow local elevation of privilege. Apply HPE Superdome Flex Server version 3.25.46 or later to resolve this issue. **CVE ID : CVE-2020-7137**	N/A	O-HPE-SUPE-010620/387
Huawei					
e6878-370_firmware					
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in some Huawei products. An unauthenticated, adjacent attacker could exploit this vulnerability to decrypt data. Successful exploitation may leak information randomly. Affected product versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T	N/A	O-HUA-E687-010620/388

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than 9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00AY Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00BX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		
Use After Free	21-05-2020	5.4	E6878-370 with versions of 10.0.3.1(H557SP27C233), 10.0.3.1(H563SP1C00), 10.0.3.1(H563SP1C233) has a use after free vulnerability. The software references memory after it has been freed in certain scenario, the attacker does a series of crafted operations through web portal, successful exploit could cause a use after free condition which may lead to malicious code execution. **CVE ID : CVE-2020-1799**	N/A	O-HUA-E687-010620/389
anne-al00_firmware					
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in some Huawei products. An unauthenticated, adjacent attacker could exploit this vulnerability to decrypt data. Successful exploitation may leak information	N/A	O-HUA-ANNE-010620/390

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			randomly. Affected product versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than 9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00AY Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00BX Versions earlier than		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		
berkeley-l09_firmware					
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in some Huawei products. An unauthenticated, adjacent attacker could exploit this vulnerability to decrypt data. Successful exploitation	N/A	O-HUA-BERK-010620/391

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may leak information randomly. Affected product versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than 9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00AY Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00BX Versions		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier than 10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		
cd17-16_firmware					
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in some Huawei products. An unauthenticated, adjacent attacker could exploit this vulnerability to decrypt	N/A	O-HUA-CD17-010620/392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			data. Successful exploitation may leak information randomly. Affected product versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than 9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00AY Versions earlier than 10.0.0.158(C00E64R1P9);		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Marie-AL00BX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		
cd18-16_firmware					
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in some Huawei products. An unauthenticated, adjacent attacker could exploit this	N/A	O-HUA-CD18-010620/393

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to decrypt data. Successful exploitation may leak information randomly. Affected product versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than 9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00AY Versions earlier than		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.0.0.158(C00E64R1P9); Marie-AL00BX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		
columbia-tl00b_firmware					
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in some Huawei products. An unauthenticated, adjacent	N/A	O-HUA-COLU-010620/394

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability to decrypt data. Successful exploitation may leak information randomly. Affected product versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than 9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00AY Versions		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier than 10.0.0.158(C00E64R1P9); Marie-AL00BX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		
lelandp-l22a_firmware					
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in some Huawei products. An	N/A	O-HUA-LELA-010620/395

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, adjacent attacker could exploit this vulnerability to decrypt data. Successful exploitation may leak information randomly. Affected product versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than 9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than 10.0.0.158(C00E64R1P9);		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Marie-AL00AY Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00BX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		
tc5200-16_firmware					
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in	N/A	O-HUA-TC52-010620/396

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			some Huawei products. An unauthenticated, adjacent attacker could exploit this vulnerability to decrypt data. Successful exploitation may leak information randomly. Affected product versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than 9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.0.0.158(C00E64R1P9); Marie-AL00AY Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00BX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		
ws5200-16_firmware					
Information	21-05-2020	3.3	There is an information	N/A	O-HUA-WS52-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			leakage vulnerability in some Huawei products. An unauthenticated, adjacent attacker could exploit this vulnerability to decrypt data. Successful exploitation may leak information randomly. Affected product versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than 9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions		010620/397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier than 10.0.0.158(C00E64R1P9); Marie-AL00AY Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00BX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		
ws5200-17_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in some Huawei products. An unauthenticated, adjacent attacker could exploit this vulnerability to decrypt data. Successful exploitation may leak information randomly. Affected product versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than 9.1.0.166(C675E5R1P4T8);	N/A	O-HUA-WS52-010620/398

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Marie-AL00AX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00AY Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00BX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ws5800-10_firmware					
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in some Huawei products. An unauthenticated, adjacent attacker could exploit this vulnerability to decrypt data. Successful exploitation may leak information randomly. Affected product versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than	N/A	O-HUA-WS58-010620/399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00AY Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00BX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ws6500-16_firmware					
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in some Huawei products. An unauthenticated, adjacent attacker could exploit this vulnerability to decrypt data. Successful exploitation may leak information randomly. Affected product versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than	N/A	O-HUA-WS65-010620/400

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00AY Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00BX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
honor_10_lite_firmware					
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in some Huawei products. An unauthenticated, adjacent attacker could exploit this vulnerability to decrypt data. Successful exploitation may leak information randomly. Affected product versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than	N/A	O-HUA-HONO-010620/401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00AY Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00BX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
cd16-10_firmware					
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in some Huawei products. An unauthenticated, adjacent attacker could exploit this vulnerability to decrypt data. Successful exploitation may leak information randomly. Affected product versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than	N/A	O-HUA-CD16-010620/402

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00AY Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00BX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
cd17-10_firmware					
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in some Huawei products. An unauthenticated, adjacent attacker could exploit this vulnerability to decrypt data. Successful exploitation may leak information randomly. Affected product versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than	N/A	O-HUA-CD17-010620/403

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00AY Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00BX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
cd18-10_firmware					
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in some Huawei products. An unauthenticated, adjacent attacker could exploit this vulnerability to decrypt data. Successful exploitation may leak information randomly. Affected product versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than	N/A	O-HUA-CD18-010620/404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00AY Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00BX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ws5200-11_firmware					
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in some Huawei products. An unauthenticated, adjacent attacker could exploit this vulnerability to decrypt data. Successful exploitation may leak information randomly. Affected product versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than	N/A	O-HUA-WS52-010620/405

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00AY Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00BX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
p30_firmware					
Improper Authentication	29-05-2020	2.1	HUAWEI P30 smartphones with versions earlier than 10.1.0.135(C00E135R2P11) have an improper authentication vulnerability. A logic error occurs when handling NFC work, an attacker should establish a NFC connection to the target phone, and then do a series of operations on the target phone. Successful exploit could allow a guest user do certain operation which is beyond the guest user's privilege. **CVE ID : CVE-2020-1798**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200527-02-smartphone-en	O-HUA-P30_-010620/406
ws6500-10_firmware					
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in some Huawei products. An unauthenticated, adjacent attacker could exploit this vulnerability to decrypt data. Successful exploitation may leak information randomly. Affected product versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions	N/A	O-HUA-WS65-010620/407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than 9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00AY Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00BX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1);		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		
IBM					
AIX					
Improper Input Validation	19-05-2020	4.9	The Spectrum Scale 4.2.0.0 through 4.2.3.21 and 5.0.0.0 through 5.0.4.3 file system component is affected by a denial of service vulnerability in its kernel module that could allow an attacker to cause a denial of service condition on the affected system. To exploit this vulnerability, a local attacker could invoke a subset of ioctls on the Spectrum Scale device with non-valid arguments. This could allow the attacker to crash the kernel. IBM X-Force ID: 179986.	https://www.ibm.com/support/pages/node/6209002	O-IBM-AIX-010620/408

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-4411		
N/A	19-05-2020	5	The Spectrum Scale 4.2.0.0 through 4.2.3.21 and 5.0.0.0 through 5.0.4.3 file system component is affected by a denial of service security vulnerability. An attacker can force the Spectrum Scale mmfsd/mmsdrserv daemons to unexpectedly exit, impacting the functionality of the Spectrum Scale cluster and the availability of file systems managed by Spectrum Scale. IBM X-Force ID: 179987. **CVE ID : CVE-2020-4412**	https://www.ibm.com/support/pages/node/6209004	O-IBM-AIX-010620/409
i					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-05-2020	1.9	IBM i 7.2, 7.3, and 7.4 users running complex SQL statements under a specific set of circumstances may allow a local user to obtain sensitive information that they should not have access to. IBM X-Force ID: 178318. **CVE ID : CVE-2020-4345**	https://www.ibm.com/support/pages/node/6208661	O-IBM-I-010620/410
Lenovo					
m8960dnf_firmware					
Improper Input Validation	28-05-2020	7.8	A denial of service vulnerability was reported in the firmware prior to version 1.01 used in Lenovo Printer LJ4010DN that could be triggered by a remote user sending a crafted packet to the device, causing an error to be	https://iknow.lenovo.com.cn/detail/dc_188830.html	O-LEN-M896-010620/411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			displayed and preventing printer from functioning until the printer is rebooted. **CVE ID : CVE-2020-8329**		
Improper Input Validation	28-05-2020	7.8	A denial of service vulnerability was reported in the firmware prior to version 1.01 used in Lenovo Printer LJ4010DN that could be triggered by a remote user sending a crafted packet to the device, preventing subsequent print jobs until the printer is rebooted. **CVE ID : CVE-2020-8330**	https://iknow.lenovo.com.cn/detail/dc_188830.html	O-LEN-M896-010620/412
lj4010dn_firmware					
Improper Input Validation	28-05-2020	7.8	A denial of service vulnerability was reported in the firmware prior to version 1.01 used in Lenovo Printer LJ4010DN that could be triggered by a remote user sending a crafted packet to the device, causing an error to be displayed and preventing printer from functioning until the printer is rebooted. **CVE ID : CVE-2020-8329**	https://iknow.lenovo.com.cn/detail/dc_188830.html	O-LEN-LJ40-010620/413
Improper Input Validation	28-05-2020	7.8	A denial of service vulnerability was reported in the firmware prior to version 1.01 used in Lenovo Printer LJ4010DN that could be triggered by a remote user sending a	https://iknow.lenovo.com.cn/detail/dc_188830.html	O-LEN-LJ40-010620/414

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted packet to the device, preventing subsequent print jobs until the printer is rebooted. **CVE ID : CVE-2020-8330**		
lj6700dn_firmware					
Improper Input Validation	28-05-2020	7.8	A denial of service vulnerability was reported in the firmware prior to version 1.01 used in Lenovo Printer LJ4010DN that could be triggered by a remote user sending a crafted packet to the device, causing an error to be displayed and preventing printer from functioning until the printer is rebooted. **CVE ID : CVE-2020-8329**	https://iknow.lenovo.com.cn/detail/dc_188830.html	O-LEN-LJ67-010620/415
Improper Input Validation	28-05-2020	7.8	A denial of service vulnerability was reported in the firmware prior to version 1.01 used in Lenovo Printer LJ4010DN that could be triggered by a remote user sending a crafted packet to the device, preventing subsequent print jobs until the printer is rebooted. **CVE ID : CVE-2020-8330**	https://iknow.lenovo.com.cn/detail/dc_188830.html	O-LEN-LJ67-010620/416
Linux					
linux_kernel					
Improper Privilege Management	22-05-2020	7.5	An Elevation of Privilege issue was discovered in Aviatrix VPN Client before 2.10.7, because of an	N/A	O-LIN-LINU-010620/417

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			incomplete fix for CVE-2020-7224. This affects Linux, macOS, and Windows installations for certain OpenSSL parameters. **CVE ID : CVE-2020-13417**		
NULL Pointer Dereference	22-05-2020	5	A NULL pointer dereference flaw was found in the Linux kernel's SELinux subsystem in versions before 5.7. This flaw occurs while importing the Commercial IP Security Option (CIPSO) protocol's category bitmap into the SELinux extensible bitmap via the' ebitmap_netlbl_import' routine. While processing the CIPSO restricted bitmap tag in the 'cipso_v4_parsetag_rbm' routine, it sets the security attribute to indicate that the category bitmap is present, even if it has not been allocated. This issue leads to a NULL pointer dereference issue while importing the same category bitmap into SELinux. This flaw allows a remote network user to crash the system kernel, resulting in a denial of service. **CVE ID : CVE-2020-10711**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10711, https://www.openwall.com/lists/oss-security/2020/05/12/2	O-LIN-LINU-010620/418
Out-of-bounds Read	18-05-2020	4.3	gadget_dev_desc_UDC_store in drivers/usb/gadget/configfs.c in the Linux kernel through 5.6.13 relies on	N/A	O-LIN-LINU-010620/419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			kstrdup without considering the possibility of an internal '\0' value, which allows attackers to trigger an out-of-bounds read, aka CID-15753588bcd4. **CVE ID : CVE-2020-13143**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-05-2020	6.5	VMware Cloud Director 10.0.x before 10.0.0.2, 9.7.0.x before 9.7.0.5, 9.5.0.x before 9.5.0.6, and 9.1.0.x before 9.1.0.4 do not properly handle input leading to a code injection vulnerability. An authenticated actor may be able to send malicious traffic to VMware Cloud Director which may lead to arbitrary remote code execution. This vulnerability can be exploited through the HTML5- and Flex-based UIs, the API Explorer interface and API access. **CVE ID : CVE-2020-3956**	N/A	O-LIN-LINU-010620/420
Improper Input Validation	19-05-2020	4.9	The Spectrum Scale 4.2.0.0 through 4.2.3.21 and 5.0.0.0 through 5.0.4.3 file system component is affected by a denial of service vulnerability in its kernel module that could allow an attacker to cause a denial of service condition on the affected system. To exploit this vulnerability, a local attacker could invoke a	https://www.ibm.com/support/pages/node/6209002	O-LIN-LINU-010620/421

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			subset of ioctls on the Spectrum Scale device with non-valid arguments. This could allow the attacker to crash the kernel. IBM X-Force ID: 179986. **CVE ID : CVE-2020-4411**		
N/A	19-05-2020	5	The Spectrum Scale 4.2.0.0 through 4.2.3.21 and 5.0.0.0 through 5.0.4.3 file system component is affected by a denial of service security vulnerability. An attacker can force the Spectrum Scale mmfsd/mmsdrserv daemons to unexpectedly exit, impacting the functionality of the Spectrum Scale cluster and the availability of file systems managed by Spectrum Scale. IBM X-Force ID: 179987. **CVE ID : CVE-2020-4412**	https://www.ibm.com/support/pages/node/6209004	O-LIN-LINU-010620/422
Microsoft					
windows					
Improper Privilege Management	22-05-2020	7.5	An Elevation of Privilege issue was discovered in Aviatrix VPN Client before 2.10.7, because of an incomplete fix for CVE-2020-7224. This affects Linux, macOS, and Windows installations for certain OpenSSL parameters. **CVE ID : CVE-2020-13417**	N/A	O-MIC-WIND-010620/423
Improper Input	26-05-2020	7.5	The Firefox content processes did not sufficiently lockdown access	N/A	O-MIC-WIND-010620/424

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			control which could result in a sandbox escape. *Note: this issue only affects Firefox on Windows operating systems.*. This vulnerability affects Firefox ESR < 68.8 and Firefox < 76. **CVE ID : CVE-2020-12388**		
Improper Input Validation	26-05-2020	7.5	The Firefox content processes did not sufficiently lockdown access control which could result in a sandbox escape. *Note: this issue only affects Firefox on Windows operating systems.*. This vulnerability affects Firefox ESR < 68.8 and Firefox < 76. **CVE ID : CVE-2020-12389**	N/A	O-MIC-WIND-010620/425
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	26-05-2020	4.6	The 'Copy as cURL' feature of Devtools' network tab did not properly escape the HTTP method of a request, which can be controlled by the website. If a user used the 'Copy as cURL' feature and pasted the command into a terminal, it could have resulted in command injection and arbitrary command execution. *Note: this issue only affects Firefox on Windows operating systems.*. This vulnerability affects Firefox ESR < 68.8, Firefox < 76, and Thunderbird < 68.8.0. **CVE ID : CVE-2020-12393**	N/A	O-MIC-WIND-010620/426
Download of	28-05-2020	7.5	Ezhttptrans.ocx ActiveX	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Code Without Integrity Check			Control in Kaoni ezHTTPTrans 1.0.0.70 and prior versions contain a vulnerability that could allow remote attacker to download arbitrary file by setting the arguments to the activex method. This can be leveraged for code execution by rebooting the victim's PC. **CVE ID : CVE-2020-7812**		010620/427
windows_8.0					
Argument Injection or Modification	21-05-2020	7.5	In RAONWIZ K Upload v2018.0.2.51 and prior, automatic update processing without integrity check on update module(web.js) allows an attacker to modify arguments which causes downloading a random DLL and injection on it. **CVE ID : CVE-2020-7808**	https://www.boho.or.kr/krcert/secNoticeView.do?bulletin_writing_sequence=35424	O-MIC-WIND-010620/428
windows_10					
Information Exposure	21-05-2020	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1141, CVE-2020-1145, CVE-2020-1179. **CVE ID : CVE-2020-0963**	N/A	O-MIC-WIND-010620/429
Improper Privilege	21-05-2020	7.2	An elevation of privilege vulnerability exists when	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			the Windows Print Spooler service improperly allows arbitrary writing to the file system, aka 'Windows Print Spooler Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1070. **CVE ID : CVE-2020-1048**		010620/430
Improper Privilege Management	21-05-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164. **CVE ID : CVE-2020-1156**	N/A	O-MIC-WIND-010620/431
Improper Privilege Management	21-05-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-	N/A	O-MIC-WIND-010620/432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-1158, CVE-2020-1164. **CVE ID : CVE-2020-1157**		
Improper Privilege Management	21-05-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1164. **CVE ID : CVE-2020-1158**	N/A	O-MIC-WIND-010620/433
Improper Input Validation	21-05-2020	5	A denial of service vulnerability exists when Hyper-V on a Windows Server fails to properly handle specially crafted network packets.To exploit the vulnerability, an attacker would send specially crafted network packets to the Hyper-V Server.The security update addresses the vulnerability by resolving the conditions where Hyper-V would fail to properly handle these network packets., aka 'Windows Hyper-V Denial of Service Vulnerability'. **CVE ID : CVE-2020-0909**	N/A	O-MIC-WIND-010620/434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists in Windows Block Level Backup Engine Service (wbengine) that allows file deletion in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1068, CVE-2020-1079. **CVE ID : CVE-2020-1010**	N/A	O-MIC-WIND-010620/435
Improper Privilege Management	21-05-2020	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-2020-1082, CVE-2020-1088. **CVE ID : CVE-2020-1021**	N/A	O-MIC-WIND-010620/436
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1126, CVE-2020-1136, CVE-2020-1150. **CVE ID : CVE-2020-1028**	N/A	O-MIC-WIND-010620/437
Improper	21-05-2020	7.6	A remote code execution	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1058, CVE-2020-1060, CVE-2020-1093. **CVE ID : CVE-2020-1035**		010620/438
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. **CVE ID : CVE-2020-1037**	N/A	O-MIC-WIND-010620/439
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1174, CVE-2020-1175, CVE-2020-1176. **CVE ID : CVE-2020-1051**	N/A	O-MIC-WIND-010620/440
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of	N/A	O-MIC-WIND-010620/441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1143. **CVE ID : CVE-2020-1054**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-05-2020	4.3	A cross-site-scripting (XSS) vulnerability exists when Active Directory Federation Services (ADFS) does not properly sanitize user inputs, aka 'Microsoft Active Directory Federation Services Cross-Site Scripting Vulnerability'. **CVE ID : CVE-2020-1055**	N/A	O-MIC-WIND-010620/442
Incorrect Permission Assignment for Critical Resource	21-05-2020	5.8	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-2020-1056**	N/A	O-MIC-WIND-010620/443
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-	N/A	O-MIC-WIND-010620/444

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1035, CVE-2020-1060, CVE-2020-1093. **CVE ID : CVE-2020-1058**		
URL Redirection to Untrusted Site ('Open Redirect')	21-05-2020	4.3	A spoofing vulnerability exists when Microsoft Edge does not properly parse HTTP content, aka 'Microsoft Edge Spoofing Vulnerability'. **CVE ID : CVE-2020-1059**	N/A	O-MIC-WIND-010620/445
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1035, CVE-2020-1058, CVE-2020-1093. **CVE ID : CVE-2020-1060**	N/A	O-MIC-WIND-010620/446
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists in the way that the Microsoft Script Runtime handles objects in memory, aka 'Microsoft Script Runtime Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1061**	N/A	O-MIC-WIND-010620/447
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory Corruption Vulnerability'. This CVE ID is unique from	N/A	O-MIC-WIND-010620/448

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-1092. **CVE ID : CVE-2020-1062**		
Improper Input Validation	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the MSHTML engine improperly validates input.An attacker could execute arbitrary code in the context of the current user, aka 'MSHTML Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1064**	N/A	O-MIC-WIND-010620/449
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	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'. **CVE ID : CVE-2020-1065**	N/A	O-MIC-WIND-010620/450
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	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-2020-1067**	N/A	O-MIC-WIND-010620/451
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists in Windows Media Service that allows file creation in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID	N/A	O-MIC-WIND-010620/452

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is unique from CVE-2020-1010, CVE-2020-1079. **CVE ID : CVE-2020-1068**		
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system, aka 'Windows Print Spooler Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1048. **CVE ID : CVE-2020-1070**	N/A	O-MIC-WIND-010620/453
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when Windows improperly handles errors tied to Remote Access Common Dialog, aka 'Windows Remote Access Common Dialog Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1071**	N/A	O-MIC-WIND-010620/454
Information Exposure	21-05-2020	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-2020-1072**	N/A	O-MIC-WIND-010620/455
Information Exposure	21-05-2020	2.1	An information disclosure vulnerability exists when Windows Subsystem for Linux improperly handles objects in memory, aka 'Windows Subsystem for Linux Information	N/A	O-MIC-WIND-010620/456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability'. **CVE ID : CVE-2020-1075**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	2.1	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. **CVE ID : CVE-2020-1076**	N/A	O-MIC-WIND-010620/457
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164. **CVE ID : CVE-2020-1077**	N/A	O-MIC-WIND-010620/458
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on the victim system, aka 'Windows Installer Elevation of Privilege Vulnerability'.	N/A	O-MIC-WIND-010620/459

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1078		
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Windows fails to properly handle objects in memory, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1010, CVE-2020-1068. **CVE ID : CVE-2020-1079**	N/A	O-MIC-WIND-010620/460
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Windows Printer Service improperly validates file paths while loading printer drivers, aka 'Windows Printer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1081**	N/A	O-MIC-WIND-010620/461
Improper Privilege Management	21-05-2020	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-2020-1021, CVE-2020-1088. **CVE ID : CVE-2020-1082**	N/A	O-MIC-WIND-010620/462
Incorrect Permission Assignment for Critical Resource	21-05-2020	2.1	A Denial Of Service vulnerability exists when Connected User Experiences and Telemetry Service fails to validate certain function values.An	N/A	O-MIC-WIND-010620/463

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker who successfully exploited this vulnerability could deny dependent security feature functionality.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 Connected User Experiences and Telemetry Service validates certain function values., aka 'Connected User Experiences and Telemetry Service Denial of Service Vulnerability'. This CVE ID is unique from CVE-2020-1123. **CVE ID : CVE-2020-1084**		
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164. **CVE ID : CVE-2020-1086**	N/A	O-MIC-WIND-010620/464

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	21-05-2020	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-2020-1114. **CVE ID : CVE-2020-1087**	N/A	O-MIC-WIND-010620/465
Improper Privilege Management	21-05-2020	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-2020-1021, CVE-2020-1082. **CVE ID : CVE-2020-1088**	N/A	O-MIC-WIND-010620/466
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164. **CVE ID : CVE-2020-1090**	N/A	O-MIC-WIND-010620/467
Improper	21-05-2020	7.6	A remote code execution	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1062. **CVE ID : CVE-2020-1092**		010620/468
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1035, CVE-2020-1058, CVE-2020-1060. **CVE ID : CVE-2020-1093**	N/A	O-MIC-WIND-010620/469
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists when Microsoft Edge PDF Reader improperly handles objects in memory, aka 'Microsoft Edge PDF Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1096**	N/A	O-MIC-WIND-010620/470
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Windows Update Stack fails to properly handle objects in memory, aka 'Windows Update Stack Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1110. **CVE ID : CVE-2020-1109**	N/A	O-MIC-WIND-010620/471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Windows Update Stack fails to properly handle objects in memory, aka 'Windows Update Stack Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1109. **CVE ID : CVE-2020-1110**	N/A	O-MIC-WIND-010620/472
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when Windows improperly handles calls to Clipboard Service, aka 'Windows Clipboard Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1121, CVE-2020-1165, CVE-2020-1166. **CVE ID : CVE-2020-1111**	N/A	O-MIC-WIND-010620/473
Unrestricted Upload of File with Dangerous Type	21-05-2020	9	An elevation of privilege vulnerability exists when the Windows Background Intelligent Transfer Service (BITS) IIS module improperly handles uploaded content, aka 'Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1112**	N/A	O-MIC-WIND-010620/474
Improper Certificate Validation	21-05-2020	9.3	A security feature bypass vulnerability exists in Microsoft Windows when the Task Scheduler service fails to properly verify	N/A	O-MIC-WIND-010620/475

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			client connections over RPC, aka 'Windows Task Scheduler Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-1113**		
Improper Privilege Management	21-05-2020	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-2020-1087. **CVE ID : CVE-2020-1114**	N/A	O-MIC-WIND-010620/476
Information Exposure	21-05-2020	2.1	An information disclosure vulnerability exists when the Windows Client Server Run-Time Subsystem (CSRSS) fails to properly handle objects in memory, aka 'Windows CSRSS Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1116**	N/A	O-MIC-WIND-010620/477
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists in the way that the Color Management Module (ICM32.dll) handles objects in memory, aka 'Microsoft Color Management Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1117**	N/A	O-MIC-WIND-010620/478
N/A	21-05-2020	7.8	A denial of service vulnerability exists in the Windows implementation of Transport Layer Security	N/A	O-MIC-WIND-010620/479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(TLS) when it improperly handles certain key exchanges, aka 'Microsoft Windows Transport Layer Security Denial of Service Vulnerability'. **CVE ID : CVE-2020-1118**		
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when Windows improperly handles calls to Clipboard Service, aka 'Windows Clipboard Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1111, CVE-2020-1165, CVE-2020-1166. **CVE ID : CVE-2020-1121**	N/A	O-MIC-WIND-010620/480
Incorrect Permission Assignment for Critical Resource	21-05-2020	2.1	A denial of service vulnerability exists when Connected User Experiences and Telemetry Service improperly handles file operations, aka 'Connected User Experiences and Telemetry Service Denial of Service Vulnerability'. This CVE ID is unique from CVE-2020-1084. **CVE ID : CVE-2020-1123**	N/A	O-MIC-WIND-010620/481
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege	N/A	O-MIC-WIND-010620/482

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. This CVE ID is unique from CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191. **CVE ID : CVE-2020-1124**		
Improper Privilege Management	21-05-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164. **CVE ID : CVE-2020-1125**	N/A	O-MIC-WIND-010620/483
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1028, CVE-2020-1136, CVE-2020-1150. **CVE ID : CVE-2020-1126**	N/A	O-MIC-WIND-010620/484
Improper	21-05-2020	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 when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191. **CVE ID : CVE-2020-1131**		010620/485
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles file and folder links, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1132**	N/A	O-MIC-WIND-010620/486
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-	N/A	O-MIC-WIND-010620/487

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191. **CVE ID : CVE-2020-1134**		
Improper Privilege Management	21-05-2020	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'. **CVE ID : CVE-2020-1135**	N/A	O-MIC-WIND-010620/488
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1028, CVE-2020-1126, CVE-2020-1150. **CVE ID : CVE-2020-1136**	N/A	O-MIC-WIND-010620/489
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists in the way the Windows Push Notification Service handles objects in memory, aka 'Windows Push Notification Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1137**	N/A	O-MIC-WIND-010620/490
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Storage Service improperly handles file operations, aka 'Windows	N/A	O-MIC-WIND-010620/491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Storage Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1138**		
Improper Privilege Management	21-05-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164. **CVE ID : CVE-2020-1139**	N/A	O-MIC-WIND-010620/492
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1140**	N/A	O-MIC-WIND-010620/493
Information Exposure	21-05-2020	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'. This CVE ID is unique from CVE-2020-	N/A	O-MIC-WIND-010620/494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0963, CVE-2020-1145, CVE-2020-1179. **CVE ID : CVE-2020-1141**		
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, aka 'Windows GDI Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1142**	N/A	O-MIC-WIND-010620/495
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1054. **CVE ID : CVE-2020-1143**	N/A	O-MIC-WIND-010620/496
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1184, CVE-2020-1185, CVE-2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-	N/A	O-MIC-WIND-010620/497

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1190, CVE-2020-1191. **CVE ID : CVE-2020-1144**		
Information Exposure	21-05-2020	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'. This CVE ID is unique from CVE-2020-0963, CVE-2020-1141, CVE-2020-1179. **CVE ID : CVE-2020-1145**	N/A	O-MIC-WIND-010620/498
Improper Privilege Management	21-05-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164. **CVE ID : CVE-2020-1149**	N/A	O-MIC-WIND-010620/499
Improper Privilege Management	21-05-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows	N/A	O-MIC-WIND-010620/500

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164. **CVE ID : CVE-2020-1151**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1153**	N/A	O-MIC-WIND-010620/501
Improper Privilege Management	21-05-2020	7.2	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-2020-1154**	N/A	O-MIC-WIND-010620/502
Improper Privilege Management	21-05-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from	N/A	O-MIC-WIND-010620/503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164. **CVE ID : CVE-2020-1155**		
Improper Privilege Management	21-05-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158. **CVE ID : CVE-2020-1164**	N/A	O-MIC-WIND-010620/504
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when Windows improperly handles calls to Clipboard Service, aka 'Windows Clipboard Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1111, CVE-2020-1121, CVE-2020-1166. **CVE ID : CVE-2020-1165**	N/A	O-MIC-WIND-010620/505
Improper Privilege	21-05-2020	7.2	An elevation of privilege vulnerability exists when	N/A	O-MIC-WIND-010620/506

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Windows improperly handles calls to Clipboard Service, aka 'Windows Clipboard Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1111, CVE-2020-1121, CVE-2020-1165. **CVE ID : CVE-2020-1166**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1051, CVE-2020-1175, CVE-2020-1176. **CVE ID : CVE-2020-1174**	N/A	O-MIC-WIND-010620/507
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1051, CVE-2020-1174, CVE-2020-1176. **CVE ID : CVE-2020-1175**	N/A	O-MIC-WIND-010620/508
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote	N/A	O-MIC-WIND-010620/509

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1051, CVE-2020-1174, CVE-2020-1175. **CVE ID : CVE-2020-1176**		
Information Exposure	21-05-2020	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0963, CVE-2020-1141, CVE-2020-1145. **CVE ID : CVE-2020-1179**	N/A	O-MIC-WIND-010620/510
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1185, CVE-2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191. **CVE ID : CVE-2020-1184**	N/A	O-MIC-WIND-010620/511
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State	N/A	O-MIC-WIND-010620/512

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191. **CVE ID : CVE-2020-1185**		
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191. **CVE ID : CVE-2020-1186**	N/A	O-MIC-WIND-010620/513
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service	N/A	O-MIC-WIND-010620/514

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-2020-1186, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191. **CVE ID : CVE-2020-1187**		
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-2020-1186, CVE-2020-1187, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191. **CVE ID : CVE-2020-1188**	N/A	O-MIC-WIND-010620/515
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-	N/A	O-MIC-WIND-010620/516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1190, CVE-2020-1191. **CVE ID : CVE-2020-1189**		
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1191. **CVE ID : CVE-2020-1190**	N/A	O-MIC-WIND-010620/517
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-2020-1186, CVE-2020-1187, CVE-	N/A	O-MIC-WIND-010620/518

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-1188, CVE-2020-1189, CVE-2020-1190. **CVE ID : CVE-2020-1191**		
Argument Injection or Modification	21-05-2020	7.5	In RAONWIZ K Upload v2018.0.2.51 and prior, automatic update processing without integrity check on update module(web.js) allows an attacker to modify arguments which causes downloading a random DLL and injection on it. **CVE ID : CVE-2020-7808**	https://www.boho.or.kr/krcert/secNoticeView.do?bulletin_writing_sequence=35424	O-MIC-WIND-010620/519
windows_7					
Information Exposure	21-05-2020	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1141, CVE-2020-1145, CVE-2020-1179. **CVE ID : CVE-2020-0963**	N/A	O-MIC-WIND-010620/520
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system, aka 'Windows Print Spooler Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1070. **CVE ID : CVE-2020-1048**	N/A	O-MIC-WIND-010620/521

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	21-05-2020	5	A denial of service vulnerability exists when Hyper-V on a Windows Server fails to properly handle specially crafted network packets.To exploit the vulnerability, an attacker would send specially crafted network packets to the Hyper-V Server.The security update addresses the vulnerability by resolving the conditions where Hyper-V would fail to properly handle these network packets., aka 'Windows Hyper-V Denial of Service Vulnerability'. **CVE ID : CVE-2020-0909**	N/A	O-MIC-WIND-010620/522
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists in Windows Block Level Backup Engine Service (wbengine) that allows file deletion in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1068, CVE-2020-1079. **CVE ID : CVE-2020-1010**	N/A	O-MIC-WIND-010620/523
Improper Restriction of Operations within the Bounds of a	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript	N/A	O-MIC-WIND-010620/524

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1058, CVE-2020-1060, CVE-2020-1093. **CVE ID : CVE-2020-1035**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1174, CVE-2020-1175, CVE-2020-1176. **CVE ID : CVE-2020-1051**	N/A	O-MIC-WIND-010620/525
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1143. **CVE ID : CVE-2020-1054**	N/A	O-MIC-WIND-010620/526
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1035, CVE-2020-1060, CVE-2020-1093.	N/A	O-MIC-WIND-010620/527

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1058		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1035, CVE-2020-1058, CVE-2020-1093. **CVE ID : CVE-2020-1060**	N/A	O-MIC-WIND-010620/528
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists in the way that the Microsoft Script Runtime handles objects in memory, aka 'Microsoft Script Runtime Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1061**	N/A	O-MIC-WIND-010620/529
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1092. **CVE ID : CVE-2020-1062**	N/A	O-MIC-WIND-010620/530
Improper Input Validation	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the MSHTML engine improperly validates input.An attacker could execute arbitrary code in the context of the current user, aka 'MSHTML Engine	N/A	O-MIC-WIND-010620/531

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1064**		
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists in .NET Framework which could allow an attacker to elevate their privilege level.To exploit the vulnerability, an attacker would first have to access the local machine, and then run a malicious program.The update addresses the vulnerability by correcting how .NET Framework activates COM objects., aka '.NET Framework Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1066**	N/A	O-MIC-WIND-010620/532
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	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-2020-1067**	N/A	O-MIC-WIND-010620/533
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system, aka 'Windows Print Spooler Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1048. **CVE ID : CVE-2020-1070**	N/A	O-MIC-WIND-010620/534

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when Windows improperly handles errors tied to Remote Access Common Dialog, aka 'Windows Remote Access Common Dialog Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1071**	N/A	O-MIC-WIND-010620/535
Information Exposure	21-05-2020	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-2020-1072**	N/A	O-MIC-WIND-010620/536
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	2.1	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. **CVE ID : CVE-2020-1076**	N/A	O-MIC-WIND-010620/537
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on the victim system, aka 'Windows Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1078**	N/A	O-MIC-WIND-010620/538

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Windows Printer Service improperly validates file paths while loading printer drivers, aka 'Windows Printer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1081**	N/A	O-MIC-WIND-010620/539
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1062. **CVE ID : CVE-2020-1092**	N/A	O-MIC-WIND-010620/540
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1035, CVE-2020-1058, CVE-2020-1060. **CVE ID : CVE-2020-1093**	N/A	O-MIC-WIND-010620/541
Unrestricted Upload of File with Dangerous Type	21-05-2020	9	An elevation of privilege vulnerability exists when the Windows Background Intelligent Transfer Service (BITS) IIS module improperly handles uploaded content, aka 'Windows Background	N/A	O-MIC-WIND-010620/542

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Intelligent Transfer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1112**		
Improper Certificate Validation	21-05-2020	9.3	A security feature bypass vulnerability exists in Microsoft Windows when the Task Scheduler service fails to properly verify client connections over RPC, aka 'Windows Task Scheduler Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-1113**	N/A	O-MIC-WIND-010620/543
Improper Privilege Management	21-05-2020	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-2020-1087. **CVE ID : CVE-2020-1114**	N/A	O-MIC-WIND-010620/544
Information Exposure	21-05-2020	2.1	An information disclosure vulnerability exists when the Windows Client Server Run-Time Subsystem (CSRSS) fails to properly handle objects in memory, aka 'Windows CSRSS Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1116**	N/A	O-MIC-WIND-010620/545
Information Exposure	21-05-2020	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-010620/546

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory, allowing an attacker to retrieve information from a targeted system, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0963, CVE-2020-1145, CVE-2020-1179. **CVE ID : CVE-2020-1141**		
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1054. **CVE ID : CVE-2020-1143**	N/A	O-MIC-WIND-010620/547
Improper Privilege Management	21-05-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164. **CVE ID : CVE-2020-1149**	N/A	O-MIC-WIND-010620/548
Improper	21-05-2020	6.8	A memory corruption	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1028, CVE-2020-1126, CVE-2020-1136. **CVE ID : CVE-2020-1150**		010620/549
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1153**	N/A	O-MIC-WIND-010620/550
Improper Privilege Management	21-05-2020	7.2	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-2020-1154**	N/A	O-MIC-WIND-010620/551
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1051, CVE-2020-1175, CVE-	N/A	O-MIC-WIND-010620/552

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-1176. **CVE ID : CVE-2020-1174**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1051, CVE-2020-1174, CVE-2020-1176. **CVE ID : CVE-2020-1175**	N/A	O-MIC-WIND-010620/553
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1051, CVE-2020-1174, CVE-2020-1175. **CVE ID : CVE-2020-1176**	N/A	O-MIC-WIND-010620/554
Information Exposure	21-05-2020	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0963, CVE-2020-1141, CVE-2020-1145. **CVE ID : CVE-2020-1179**	N/A	O-MIC-WIND-010620/555

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Argument Injection or Modification	21-05-2020	7.5	In RAONWIZ K Upload v2018.0.2.51 and prior, automatic update processing without integrity check on update module(web.js) allows an attacker to modify arguments which causes downloading a random DLL and injection on it. **CVE ID : CVE-2020-7808**	https://www.boho.or.kr/krcert/secNoticeView.do?bulletin_writing_sequence=35424	O-MIC-WIND-010620/556
windows_8.1					
Information Exposure	21-05-2020	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1141, CVE-2020-1145, CVE-2020-1179. **CVE ID : CVE-2020-0963**	N/A	O-MIC-WIND-010620/557
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system, aka 'Windows Print Spooler Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1070. **CVE ID : CVE-2020-1048**	N/A	O-MIC-WIND-010620/558
Improper Input Validation	21-05-2020	5	A denial of service vulnerability exists when Hyper-V on a Windows Server fails to properly	N/A	O-MIC-WIND-010620/559

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			handle specially crafted network packets.To exploit the vulnerability, an attacker would send specially crafted network packets to the Hyper-V Server.The security update addresses the vulnerability by resolving the conditions where Hyper-V would fail to properly handle these network packets., aka 'Windows Hyper-V Denial of Service Vulnerability'. **CVE ID : CVE-2020-0909**		
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists in Windows Block Level Backup Engine Service (wbengine) that allows file deletion in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1068, CVE-2020-1079. **CVE ID : CVE-2020-1010**	N/A	O-MIC-WIND-010620/560
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1058, CVE-2020-1060, CVE-	N/A	O-MIC-WIND-010620/561

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-1093. **CVE ID : CVE-2020-1035**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1174, CVE-2020-1175, CVE-2020-1176. **CVE ID : CVE-2020-1051**	N/A	O-MIC-WIND-010620/562
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1143. **CVE ID : CVE-2020-1054**	N/A	O-MIC-WIND-010620/563
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1035, CVE-2020-1060, CVE-2020-1093. **CVE ID : CVE-2020-1058**	N/A	O-MIC-WIND-010620/564
Improper Restriction of Operations	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript	N/A	O-MIC-WIND-010620/565

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1035, CVE-2020-1058, CVE-2020-1093. **CVE ID : CVE-2020-1060**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists in the way that the Microsoft Script Runtime handles objects in memory, aka 'Microsoft Script Runtime Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1061**	N/A	O-MIC-WIND-010620/566
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1092. **CVE ID : CVE-2020-1062**	N/A	O-MIC-WIND-010620/567
Improper Input Validation	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the MSHTML engine improperly validates input.An attacker could execute arbitrary code in the context of the current user, aka 'MSHTML Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1064**	N/A	O-MIC-WIND-010620/568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	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-2020-1067**	N/A	O-MIC-WIND-010620/569
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system, aka 'Windows Print Spooler Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1048. **CVE ID : CVE-2020-1070**	N/A	O-MIC-WIND-010620/570
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when Windows improperly handles errors tied to Remote Access Common Dialog, aka 'Windows Remote Access Common Dialog Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1071**	N/A	O-MIC-WIND-010620/571
Information Exposure	21-05-2020	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-2020-1072**	N/A	O-MIC-WIND-010620/572
Improper Restriction of Operations	21-05-2020	2.1	A denial of service vulnerability exists when Windows improperly	N/A	O-MIC-WIND-010620/573

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			handles objects in memory, aka 'Windows Denial of Service Vulnerability'. **CVE ID : CVE-2020-1076**		
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on the victim system, aka 'Windows Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1078**	N/A	O-MIC-WIND-010620/574
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Windows fails to properly handle objects in memory, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1010, CVE-2020-1068. **CVE ID : CVE-2020-1079**	N/A	O-MIC-WIND-010620/575
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Windows Printer Service improperly validates file paths while loading printer drivers, aka 'Windows Printer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1081**	N/A	O-MIC-WIND-010620/576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1062. **CVE ID : CVE-2020-1092**	N/A	O-MIC-WIND-010620/577
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1035, CVE-2020-1058, CVE-2020-1060. **CVE ID : CVE-2020-1093**	N/A	O-MIC-WIND-010620/578
Unrestricted Upload of File with Dangerous Type	21-05-2020	9	An elevation of privilege vulnerability exists when the Windows Background Intelligent Transfer Service (BITS) IIS module improperly handles uploaded content, aka 'Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1112**	N/A	O-MIC-WIND-010620/579
Improper Certificate Validation	21-05-2020	9.3	A security feature bypass vulnerability exists in Microsoft Windows when the Task Scheduler service fails to properly verify client connections over RPC,	N/A	O-MIC-WIND-010620/580

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			aka 'Windows Task Scheduler Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-1113**		
Improper Privilege Management	21-05-2020	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-2020-1087. **CVE ID : CVE-2020-1114**	N/A	O-MIC-WIND-010620/581
Information Exposure	21-05-2020	2.1	An information disclosure vulnerability exists when the Windows Client Server Run-Time Subsystem (CSRSS) fails to properly handle objects in memory, aka 'Windows CSRSS Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1116**	N/A	O-MIC-WIND-010620/582
Improper Privilege Management	21-05-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-	N/A	O-MIC-WIND-010620/583

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1164. **CVE ID : CVE-2020-1125**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1028, CVE-2020-1126, CVE-2020-1150. **CVE ID : CVE-2020-1136**	N/A	O-MIC-WIND-010620/584
Information Exposure	21-05-2020	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'. This CVE ID is unique from CVE-2020-0963, CVE-2020-1145, CVE-2020-1179. **CVE ID : CVE-2020-1141**	N/A	O-MIC-WIND-010620/585
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1054. **CVE ID : CVE-2020-1143**	N/A	O-MIC-WIND-010620/586

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	21-05-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164. **CVE ID : CVE-2020-1149**	N/A	O-MIC-WIND-010620/587
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1153**	N/A	O-MIC-WIND-010620/588
Improper Privilege Management	21-05-2020	7.2	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-2020-1154**	N/A	O-MIC-WIND-010620/589
Improper Restriction of Operations	21-05-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database	N/A	O-MIC-WIND-010620/590

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1051, CVE-2020-1175, CVE-2020-1176. **CVE ID : CVE-2020-1174**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1051, CVE-2020-1174, CVE-2020-1176. **CVE ID : CVE-2020-1175**	N/A	O-MIC-WIND-010620/591
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1051, CVE-2020-1174, CVE-2020-1175. **CVE ID : CVE-2020-1176**	N/A	O-MIC-WIND-010620/592
Information Exposure	21-05-2020	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI	N/A	O-MIC-WIND-010620/593

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0963, CVE-2020-1141, CVE-2020-1145. **CVE ID : CVE-2020-1179**		
windows_rt_8.1					
Information Exposure	21-05-2020	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1141, CVE-2020-1145, CVE-2020-1179. **CVE ID : CVE-2020-0963**	N/A	O-MIC-WIND-010620/594
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system, aka 'Windows Print Spooler Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1070. **CVE ID : CVE-2020-1048**	N/A	O-MIC-WIND-010620/595
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists in Windows Block Level Backup Engine Service (wbengine) that allows file deletion in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to	N/A	O-MIC-WIND-010620/596

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the system, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1068, CVE-2020-1079. **CVE ID : CVE-2020-1010**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1058, CVE-2020-1060, CVE-2020-1093. **CVE ID : CVE-2020-1035**	N/A	O-MIC-WIND-010620/597
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1174, CVE-2020-1175, CVE-2020-1176. **CVE ID : CVE-2020-1051**	N/A	O-MIC-WIND-010620/598
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from	N/A	O-MIC-WIND-010620/599

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-1143. **CVE ID : CVE-2020-1054**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1035, CVE-2020-1060, CVE-2020-1093. **CVE ID : CVE-2020-1058**	N/A	O-MIC-WIND-010620/600
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1035, CVE-2020-1058, CVE-2020-1093. **CVE ID : CVE-2020-1060**	N/A	O-MIC-WIND-010620/601
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists in the way that the Microsoft Script Runtime handles objects in memory, aka 'Microsoft Script Runtime Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1061**	N/A	O-MIC-WIND-010620/602
Improper Restriction of Operations within the Bounds of a	21-05-2020	7.6	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory	N/A	O-MIC-WIND-010620/603

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1092. **CVE ID : CVE-2020-1062**		
Improper Input Validation	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the MSHTML engine improperly validates input.An attacker could execute arbitrary code in the context of the current user, aka 'MSHTML Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1064**	N/A	O-MIC-WIND-010620/604
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	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-2020-1067**	N/A	O-MIC-WIND-010620/605
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system, aka 'Windows Print Spooler Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1048. **CVE ID : CVE-2020-1070**	N/A	O-MIC-WIND-010620/606
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when Windows improperly handles errors tied to Remote Access Common Dialog, aka 'Windows	N/A	O-MIC-WIND-010620/607

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Remote Access Common Dialog Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1071**		
Information Exposure	21-05-2020	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-2020-1072**	N/A	O-MIC-WIND-010620/608
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	2.1	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. **CVE ID : CVE-2020-1076**	N/A	O-MIC-WIND-010620/609
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on the victim system, aka 'Windows Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1078**	N/A	O-MIC-WIND-010620/610
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Windows fails to properly handle objects in memory, aka 'Microsoft Windows Elevation of	N/A	O-MIC-WIND-010620/611

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1010, CVE-2020-1068. **CVE ID : CVE-2020-1079**		
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Windows Printer Service improperly validates file paths while loading printer drivers, aka 'Windows Printer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1081**	N/A	O-MIC-WIND-010620/612
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1062. **CVE ID : CVE-2020-1092**	N/A	O-MIC-WIND-010620/613
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1035, CVE-2020-1058, CVE-2020-1060. **CVE ID : CVE-2020-1093**	N/A	O-MIC-WIND-010620/614
Unrestricted Upload of File with	21-05-2020	9	An elevation of privilege vulnerability exists when the Windows Background	N/A	O-MIC-WIND-010620/615

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			Intelligent Transfer Service (BITS) IIS module improperly handles uploaded content, aka 'Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1112**		
Improper Certificate Validation	21-05-2020	9.3	A security feature bypass vulnerability exists in Microsoft Windows when the Task Scheduler service fails to properly verify client connections over RPC, aka 'Windows Task Scheduler Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-1113**	N/A	O-MIC-WIND-010620/616
Improper Privilege Management	21-05-2020	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-2020-1087. **CVE ID : CVE-2020-1114**	N/A	O-MIC-WIND-010620/617
Information Exposure	21-05-2020	2.1	An information disclosure vulnerability exists when the Windows Client Server Run-Time Subsystem (CSRSS) fails to properly handle objects in memory, aka 'Windows CSRSS Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1116**	N/A	O-MIC-WIND-010620/618

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	21-05-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164. **CVE ID : CVE-2020-1125**	N/A	O-MIC-WIND-010620/619
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1028, CVE-2020-1126, CVE-2020-1150. **CVE ID : CVE-2020-1136**	N/A	O-MIC-WIND-010620/620
Information Exposure	21-05-2020	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'. This CVE ID is unique from CVE-2020-	N/A	O-MIC-WIND-010620/621

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0963, CVE-2020-1145, CVE-2020-1179. **CVE ID : CVE-2020-1141**		
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1054. **CVE ID : CVE-2020-1143**	N/A	O-MIC-WIND-010620/622
Improper Privilege Management	21-05-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164. **CVE ID : CVE-2020-1149**	N/A	O-MIC-WIND-010620/623
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Remote Code Execution Vulnerability'.	N/A	O-MIC-WIND-010620/624

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1153		
Improper Privilege Management	21-05-2020	7.2	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-2020-1154**	N/A	O-MIC-WIND-010620/625
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1051, CVE-2020-1175, CVE-2020-1176. **CVE ID : CVE-2020-1174**	N/A	O-MIC-WIND-010620/626
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1051, CVE-2020-1174, CVE-2020-1176. **CVE ID : CVE-2020-1175**	N/A	O-MIC-WIND-010620/627
Improper Restriction of Operations within the	21-05-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles	N/A	O-MIC-WIND-010620/628

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1051, CVE-2020-1174, CVE-2020-1175. **CVE ID : CVE-2020-1176**		
Information Exposure	21-05-2020	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0963, CVE-2020-1141, CVE-2020-1145. **CVE ID : CVE-2020-1179**	N/A	O-MIC-WIND-010620/629
windows_server_2008					
Information Exposure	21-05-2020	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1141, CVE-2020-1145, CVE-2020-1179. **CVE ID : CVE-2020-0963**	N/A	O-MIC-WIND-010620/630
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system, aka 'Windows Print	N/A	O-MIC-WIND-010620/631

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Spooler Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1070. **CVE ID : CVE-2020-1048**		
Improper Input Validation	21-05-2020	5	A denial of service vulnerability exists when Hyper-V on a Windows Server fails to properly handle specially crafted network packets.To exploit the vulnerability, an attacker would send specially crafted network packets to the Hyper-V Server.The security update addresses the vulnerability by resolving the conditions where Hyper-V would fail to properly handle these network packets., aka 'Windows Hyper-V Denial of Service Vulnerability'. **CVE ID : CVE-2020-0909**	N/A	O-MIC-WIND-010620/632
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists in Windows Block Level Backup Engine Service (wbengine) that allows file deletion in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1068, CVE-2020-1079.	N/A	O-MIC-WIND-010620/633

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1010		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1058, CVE-2020-1060, CVE-2020-1093. **CVE ID : CVE-2020-1035**	N/A	O-MIC-WIND-010620/634
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1174, CVE-2020-1175, CVE-2020-1176. **CVE ID : CVE-2020-1051**	N/A	O-MIC-WIND-010620/635
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1143. **CVE ID : CVE-2020-1054**	N/A	O-MIC-WIND-010620/636
Improper Restriction of Operations within the	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in	N/A	O-MIC-WIND-010620/637

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1035, CVE-2020-1060, CVE-2020-1093. **CVE ID : CVE-2020-1058**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1035, CVE-2020-1058, CVE-2020-1093. **CVE ID : CVE-2020-1060**	N/A	O-MIC-WIND-010620/638
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists in the way that the Microsoft Script Runtime handles objects in memory, aka 'Microsoft Script Runtime Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1061**	N/A	O-MIC-WIND-010620/639
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1092. **CVE ID : CVE-2020-1062**	N/A	O-MIC-WIND-010620/640
Improper Input	21-05-2020	7.6	A remote code execution vulnerability exists in the	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			way that the MSHTML engine improperly validates input.An attacker could execute arbitrary code in the context of the current user, aka 'MSHTML Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1064**		010620/641
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists in .NET Framework which could allow an attacker to elevate their privilege level.To exploit the vulnerability, an attacker would first have to access the local machine, and then run a malicious program.The update addresses the vulnerability by correcting how .NET Framework activates COM objects., aka '.NET Framework Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1066**	N/A	O-MIC-WIND-010620/642
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	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-2020-1067**	N/A	O-MIC-WIND-010620/643
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system, aka 'Windows Print	N/A	O-MIC-WIND-010620/644

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Spooler Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1048. **CVE ID : CVE-2020-1070**		
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when Windows improperly handles errors tied to Remote Access Common Dialog, aka 'Windows Remote Access Common Dialog Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1071**	N/A	O-MIC-WIND-010620/645
Information Exposure	21-05-2020	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-2020-1072**	N/A	O-MIC-WIND-010620/646
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	2.1	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. **CVE ID : CVE-2020-1076**	N/A	O-MIC-WIND-010620/647
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on	N/A	O-MIC-WIND-010620/648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the victim system, aka 'Windows Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1078**		
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Windows Printer Service improperly validates file paths while loading printer drivers, aka 'Windows Printer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1081**	N/A	O-MIC-WIND-010620/649
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1062. **CVE ID : CVE-2020-1092**	N/A	O-MIC-WIND-010620/650
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1035, CVE-2020-1058, CVE-2020-1060. **CVE ID : CVE-2020-1093**	N/A	O-MIC-WIND-010620/651
Unrestricted Upload of File with	21-05-2020	9	An elevation of privilege vulnerability exists when the Windows Background	N/A	O-MIC-WIND-010620/652

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			Intelligent Transfer Service (BITS) IIS module improperly handles uploaded content, aka 'Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1112**		
Improper Certificate Validation	21-05-2020	9.3	A security feature bypass vulnerability exists in Microsoft Windows when the Task Scheduler service fails to properly verify client connections over RPC, aka 'Windows Task Scheduler Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-1113**	N/A	O-MIC-WIND-010620/653
Improper Privilege Management	21-05-2020	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-2020-1087. **CVE ID : CVE-2020-1114**	N/A	O-MIC-WIND-010620/654
Information Exposure	21-05-2020	2.1	An information disclosure vulnerability exists when the Windows Client Server Run-Time Subsystem (CSRSS) fails to properly handle objects in memory, aka 'Windows CSRSS Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1116**	N/A	O-MIC-WIND-010620/655

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	21-05-2020	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'. This CVE ID is unique from CVE-2020-0963, CVE-2020-1145, CVE-2020-1179. **CVE ID : CVE-2020-1141**	N/A	O-MIC-WIND-010620/656
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1054. **CVE ID : CVE-2020-1143**	N/A	O-MIC-WIND-010620/657
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1028, CVE-2020-1126, CVE-2020-1136. **CVE ID : CVE-2020-1150**	N/A	O-MIC-WIND-010620/658
Improper Restriction of	21-05-2020	9.3	A remote code execution vulnerability exists in the	N/A	O-MIC-WIND-010620/659

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1153**		
Improper Privilege Management	21-05-2020	7.2	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-2020-1154**	N/A	O-MIC-WIND-010620/660
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1051, CVE-2020-1175, CVE-2020-1176. **CVE ID : CVE-2020-1174**	N/A	O-MIC-WIND-010620/661
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1051, CVE-2020-1174, CVE-	N/A	O-MIC-WIND-010620/662

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-1176. **CVE ID : CVE-2020-1175**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1051, CVE-2020-1174, CVE-2020-1175. **CVE ID : CVE-2020-1176**	N/A	O-MIC-WIND-010620/663
Information Exposure	21-05-2020	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0963, CVE-2020-1141, CVE-2020-1145. **CVE ID : CVE-2020-1179**	N/A	O-MIC-WIND-010620/664
windows_server_2012					
Information Exposure	21-05-2020	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1141, CVE-2020-1145, CVE-2020-1179.	N/A	O-MIC-WIND-010620/665

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0963		
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system, aka 'Windows Print Spooler Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1070. **CVE ID : CVE-2020-1048**	N/A	O-MIC-WIND-010620/666
Improper Input Validation	21-05-2020	5	A denial of service vulnerability exists when Hyper-V on a Windows Server fails to properly handle specially crafted network packets.To exploit the vulnerability, an attacker would send specially crafted network packets to the Hyper-V Server.The security update addresses the vulnerability by resolving the conditions where Hyper-V would fail to properly handle these network packets., aka 'Windows Hyper-V Denial of Service Vulnerability'. **CVE ID : CVE-2020-0909**	N/A	O-MIC-WIND-010620/667
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists in Windows Block Level Backup Engine Service (wbengine) that allows file deletion in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to	N/A	O-MIC-WIND-010620/668

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the system, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1068, CVE-2020-1079. **CVE ID : CVE-2020-1010**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1058, CVE-2020-1060, CVE-2020-1093. **CVE ID : CVE-2020-1035**	N/A	O-MIC-WIND-010620/669
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1174, CVE-2020-1175, CVE-2020-1176. **CVE ID : CVE-2020-1051**	N/A	O-MIC-WIND-010620/670
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from	N/A	O-MIC-WIND-010620/671

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-1143. **CVE ID : CVE-2020-1054**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1035, CVE-2020-1060, CVE-2020-1093. **CVE ID : CVE-2020-1058**	N/A	O-MIC-WIND-010620/672
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1035, CVE-2020-1058, CVE-2020-1093. **CVE ID : CVE-2020-1060**	N/A	O-MIC-WIND-010620/673
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists in the way that the Microsoft Script Runtime handles objects in memory, aka 'Microsoft Script Runtime Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1061**	N/A	O-MIC-WIND-010620/674
Improper Restriction of Operations within the Bounds of a	21-05-2020	7.6	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory	N/A	O-MIC-WIND-010620/675

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1092. **CVE ID : CVE-2020-1062**		
Improper Input Validation	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the MSHTML engine improperly validates input.An attacker could execute arbitrary code in the context of the current user, aka 'MSHTML Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1064**	N/A	O-MIC-WIND-010620/676
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	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-2020-1067**	N/A	O-MIC-WIND-010620/677
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system, aka 'Windows Print Spooler Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1048. **CVE ID : CVE-2020-1070**	N/A	O-MIC-WIND-010620/678
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when Windows improperly handles errors tied to Remote Access Common Dialog, aka 'Windows	N/A	O-MIC-WIND-010620/679

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Remote Access Common Dialog Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1071**		
Information Exposure	21-05-2020	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-2020-1072**	N/A	O-MIC-WIND-010620/680
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	2.1	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. **CVE ID : CVE-2020-1076**	N/A	O-MIC-WIND-010620/681
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on the victim system, aka 'Windows Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1078**	N/A	O-MIC-WIND-010620/682
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Windows fails to properly handle objects in memory, aka 'Microsoft Windows Elevation of	N/A	O-MIC-WIND-010620/683

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1010, CVE-2020-1068. **CVE ID : CVE-2020-1079**		
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Windows Printer Service improperly validates file paths while loading printer drivers, aka 'Windows Printer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1081**	N/A	O-MIC-WIND-010620/684
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1062. **CVE ID : CVE-2020-1092**	N/A	O-MIC-WIND-010620/685
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1035, CVE-2020-1058, CVE-2020-1060. **CVE ID : CVE-2020-1093**	N/A	O-MIC-WIND-010620/686
Unrestricted Upload of File with	21-05-2020	9	An elevation of privilege vulnerability exists when the Windows Background	N/A	O-MIC-WIND-010620/687

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			Intelligent Transfer Service (BITS) IIS module improperly handles uploaded content, aka 'Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1112**		
Improper Certificate Validation	21-05-2020	9.3	A security feature bypass vulnerability exists in Microsoft Windows when the Task Scheduler service fails to properly verify client connections over RPC, aka 'Windows Task Scheduler Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-1113**	N/A	O-MIC-WIND-010620/688
Improper Privilege Management	21-05-2020	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-2020-1087. **CVE ID : CVE-2020-1114**	N/A	O-MIC-WIND-010620/689
Information Exposure	21-05-2020	2.1	An information disclosure vulnerability exists when the Windows Client Server Run-Time Subsystem (CSRSS) fails to properly handle objects in memory, aka 'Windows CSRSS Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1116**	N/A	O-MIC-WIND-010620/690

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1028, CVE-2020-1126, CVE-2020-1150. **CVE ID : CVE-2020-1136**	N/A	O-MIC-WIND-010620/691
Information Exposure	21-05-2020	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'. This CVE ID is unique from CVE-2020-0963, CVE-2020-1145, CVE-2020-1179. **CVE ID : CVE-2020-1141**	N/A	O-MIC-WIND-010620/692
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1054. **CVE ID : CVE-2020-1143**	N/A	O-MIC-WIND-010620/693
Improper Privilege	21-05-2020	6.8	An elevation of privilege vulnerability exists when	N/A	O-MIC-WIND-010620/694

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164. **CVE ID : CVE-2020-1149**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1153**	N/A	O-MIC-WIND-010620/695
Improper Privilege Management	21-05-2020	7.2	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-2020-1154**	N/A	O-MIC-WIND-010620/696
Improper Restriction of Operations within the Bounds of a	21-05-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet	N/A	O-MIC-WIND-010620/697

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1051, CVE-2020-1175, CVE-2020-1176. **CVE ID : CVE-2020-1174**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1051, CVE-2020-1174, CVE-2020-1176. **CVE ID : CVE-2020-1175**	N/A	O-MIC-WIND-010620/698
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1051, CVE-2020-1174, CVE-2020-1175. **CVE ID : CVE-2020-1176**	N/A	O-MIC-WIND-010620/699
Information Exposure	21-05-2020	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID	N/A	O-MIC-WIND-010620/700

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is unique from CVE-2020-0963, CVE-2020-1141, CVE-2020-1145. **CVE ID : CVE-2020-1179**		
windows_server_2016					
Information Exposure	21-05-2020	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1141, CVE-2020-1145, CVE-2020-1179. **CVE ID : CVE-2020-0963**	N/A	O-MIC-WIND-010620/701
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system, aka 'Windows Print Spooler Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1070. **CVE ID : CVE-2020-1048**	N/A	O-MIC-WIND-010620/702
Improper Privilege Management	21-05-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-	N/A	O-MIC-WIND-010620/703

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164. **CVE ID : CVE-2020-1156**		
Improper Privilege Management	21-05-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1158, CVE-2020-1164. **CVE ID : CVE-2020-1157**	N/A	O-MIC-WIND-010620/704
Improper Privilege Management	21-05-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1164.	N/A	O-MIC-WIND-010620/705

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1158		
Improper Input Validation	21-05-2020	5	A denial of service vulnerability exists when Hyper-V on a Windows Server fails to properly handle specially crafted network packets.To exploit the vulnerability, an attacker would send specially crafted network packets to the Hyper-V Server.The security update addresses the vulnerability by resolving the conditions where Hyper-V would fail to properly handle these network packets., aka 'Windows Hyper-V Denial of Service Vulnerability'. **CVE ID : CVE-2020-0909**	N/A	O-MIC-WIND-010620/706
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists in Windows Block Level Backup Engine Service (wbengine) that allows file deletion in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1068, CVE-2020-1079. **CVE ID : CVE-2020-1010**	N/A	O-MIC-WIND-010620/707
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles	N/A	O-MIC-WIND-010620/708

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1082, CVE-2020-1088. **CVE ID : CVE-2020-1021**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1126, CVE-2020-1136, CVE-2020-1150. **CVE ID : CVE-2020-1028**	N/A	O-MIC-WIND-010620/709
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1058, CVE-2020-1060, CVE-2020-1093. **CVE ID : CVE-2020-1035**	N/A	O-MIC-WIND-010620/710
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. **CVE ID : CVE-2020-1037**	N/A	O-MIC-WIND-010620/711

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1174, CVE-2020-1175, CVE-2020-1176. **CVE ID : CVE-2020-1051**	N/A	O-MIC-WIND-010620/712
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1143. **CVE ID : CVE-2020-1054**	N/A	O-MIC-WIND-010620/713
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-05-2020	4.3	A cross-site-scripting (XSS) vulnerability exists when Active Directory Federation Services (ADFS) does not properly sanitize user inputs, aka 'Microsoft Active Directory Federation Services Cross-Site Scripting Vulnerability'. **CVE ID : CVE-2020-1055**	N/A	O-MIC-WIND-010620/714
Incorrect Permission Assignment for Critical Resource	21-05-2020	5.8	An elevation of privilege vulnerability exists when Microsoft Edge does not properly enforce cross-domain policies, which could allow an attacker to	N/A	O-MIC-WIND-010620/715

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2020-1056**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1035, CVE-2020-1060, CVE-2020-1093. **CVE ID : CVE-2020-1058**	N/A	O-MIC-WIND-010620/716
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1035, CVE-2020-1058, CVE-2020-1093. **CVE ID : CVE-2020-1060**	N/A	O-MIC-WIND-010620/717
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists in the way that the Microsoft Script Runtime handles objects in memory, aka 'Microsoft Script Runtime	N/A	O-MIC-WIND-010620/718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1061**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1092. **CVE ID : CVE-2020-1062**	N/A	O-MIC-WIND-010620/719
Improper Input Validation	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the MSHTML engine improperly validates input.An attacker could execute arbitrary code in the context of the current user, aka 'MSHTML Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1064**	N/A	O-MIC-WIND-010620/720
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	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-2020-1067**	N/A	O-MIC-WIND-010620/721
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists in Windows Media Service that allows file creation in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka	N/A	O-MIC-WIND-010620/722

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1010, CVE-2020-1079. **CVE ID : CVE-2020-1068**		
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system, aka 'Windows Print Spooler Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1048. **CVE ID : CVE-2020-1070**	N/A	O-MIC-WIND-010620/723
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when Windows improperly handles errors tied to Remote Access Common Dialog, aka 'Windows Remote Access Common Dialog Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1071**	N/A	O-MIC-WIND-010620/724
Information Exposure	21-05-2020	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-2020-1072**	N/A	O-MIC-WIND-010620/725
Information Exposure	21-05-2020	2.1	An information disclosure vulnerability exists when Windows Subsystem for Linux improperly handles	N/A	O-MIC-WIND-010620/726

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			objects in memory, aka 'Windows Subsystem for Linux Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1075**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	2.1	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. **CVE ID : CVE-2020-1076**	N/A	O-MIC-WIND-010620/727
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164. **CVE ID : CVE-2020-1077**	N/A	O-MIC-WIND-010620/728
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on the victim system, aka	N/A	O-MIC-WIND-010620/729

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			'Windows Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1078**		
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Windows fails to properly handle objects in memory, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1010, CVE-2020-1068. **CVE ID : CVE-2020-1079**	N/A	O-MIC-WIND-010620/730
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Windows Printer Service improperly validates file paths while loading printer drivers, aka 'Windows Printer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1081**	N/A	O-MIC-WIND-010620/731
Improper Privilege Management	21-05-2020	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-2020-1021, CVE-2020-1088. **CVE ID : CVE-2020-1082**	N/A	O-MIC-WIND-010620/732
Incorrect Permission Assignment for	21-05-2020	2.1	A Denial Of Service vulnerability exists when Connected User	N/A	O-MIC-WIND-010620/733

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Critical Resource			Experiences and Telemetry Service fails to validate certain function values.An attacker who successfully exploited this vulnerability could deny dependent security feature functionality.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 Connected User Experiences and Telemetry Service validates certain function values., aka 'Connected User Experiences and Telemetry Service Denial of Service Vulnerability'. This CVE ID is unique from CVE-2020-1123. **CVE ID : CVE-2020-1084**		
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-	N/A	O-MIC-WIND-010620/734

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1164. **CVE ID : CVE-2020-1086**		
Improper Privilege Management	21-05-2020	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-2020-1114. **CVE ID : CVE-2020-1087**	N/A	O-MIC-WIND-010620/735
Improper Privilege Management	21-05-2020	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-2020-1021, CVE-2020-1082. **CVE ID : CVE-2020-1088**	N/A	O-MIC-WIND-010620/736
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164.	N/A	O-MIC-WIND-010620/737

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1090		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1062. **CVE ID : CVE-2020-1092**	N/A	O-MIC-WIND-010620/738
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1035, CVE-2020-1058, CVE-2020-1060. **CVE ID : CVE-2020-1093**	N/A	O-MIC-WIND-010620/739
Unrestricted Upload of File with Dangerous Type	21-05-2020	9	An elevation of privilege vulnerability exists when the Windows Background Intelligent Transfer Service (BITS) IIS module improperly handles uploaded content, aka 'Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1112**	N/A	O-MIC-WIND-010620/740
Improper Certificate Validation	21-05-2020	9.3	A security feature bypass vulnerability exists in Microsoft Windows when the Task Scheduler service fails to properly verify	N/A	O-MIC-WIND-010620/741

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			client connections over RPC, aka 'Windows Task Scheduler Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-1113**		
Improper Privilege Management	21-05-2020	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-2020-1087. **CVE ID : CVE-2020-1114**	N/A	O-MIC-WIND-010620/742
Information Exposure	21-05-2020	2.1	An information disclosure vulnerability exists when the Windows Client Server Run-Time Subsystem (CSRSS) fails to properly handle objects in memory, aka 'Windows CSRSS Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1116**	N/A	O-MIC-WIND-010620/743
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists in the way that the Color Management Module (ICM32.dll) handles objects in memory, aka 'Microsoft Color Management Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1117**	N/A	O-MIC-WIND-010620/744
Incorrect Permission Assignment for Critical	21-05-2020	2.1	A denial of service vulnerability exists when Connected User Experiences and Telemetry	N/A	O-MIC-WIND-010620/745

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource			Service improperly handles file operations, aka 'Connected User Experiences and Telemetry Service Denial of Service Vulnerability'. This CVE ID is unique from CVE-2020-1084. **CVE ID : CVE-2020-1123**		
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191. **CVE ID : CVE-2020-1124**	N/A	O-MIC-WIND-010620/746
Improper Privilege Management	21-05-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-	N/A	O-MIC-WIND-010620/747

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164. **CVE ID : CVE-2020-1125**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1028, CVE-2020-1136, CVE-2020-1150. **CVE ID : CVE-2020-1126**	N/A	O-MIC-WIND-010620/748
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191. **CVE ID : CVE-2020-1131**	N/A	O-MIC-WIND-010620/749
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles file and folder links, aka 'Windows Error	N/A	O-MIC-WIND-010620/750

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Reporting Manager Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1132**		
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191. **CVE ID : CVE-2020-1134**	N/A	O-MIC-WIND-010620/751
Improper Privilege Management	21-05-2020	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'. **CVE ID : CVE-2020-1135**	N/A	O-MIC-WIND-010620/752
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from	N/A	O-MIC-WIND-010620/753

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-1028, CVE-2020-1126, CVE-2020-1150. **CVE ID : CVE-2020-1136**		
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists in the way the Windows Push Notification Service handles objects in memory, aka 'Windows Push Notification Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1137**	N/A	O-MIC-WIND-010620/754
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Storage Service improperly handles file operations, aka 'Windows Storage Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1138**	N/A	O-MIC-WIND-010620/755
Improper Privilege Management	21-05-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164. **CVE ID : CVE-2020-1139**	N/A	O-MIC-WIND-010620/756
Improper Privilege	21-05-2020	7.2	An elevation of privilege vulnerability exists when	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1140**		010620/757
Information Exposure	21-05-2020	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'. This CVE ID is unique from CVE-2020-0963, CVE-2020-1145, CVE-2020-1179. **CVE ID : CVE-2020-1141**	N/A	O-MIC-WIND-010620/758
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, aka 'Windows GDI Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1142**	N/A	O-MIC-WIND-010620/759
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1054.	N/A	O-MIC-WIND-010620/760

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1143		
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1184, CVE-2020-1185, CVE-2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191. **CVE ID : CVE-2020-1144**	N/A	O-MIC-WIND-010620/761
Information Exposure	21-05-2020	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'. This CVE ID is unique from CVE-2020-0963, CVE-2020-1141, CVE-2020-1179. **CVE ID : CVE-2020-1145**	N/A	O-MIC-WIND-010620/762
Improper Privilege Management	21-05-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of	N/A	O-MIC-WIND-010620/763

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164. **CVE ID : CVE-2020-1149**		
Improper Privilege Management	21-05-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164. **CVE ID : CVE-2020-1151**	N/A	O-MIC-WIND-010620/764
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1153**	N/A	O-MIC-WIND-010620/765
Improper Privilege	21-05-2020	7.2	An elevation of privilege vulnerability exists when	N/A	O-MIC-WIND-010620/766

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			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-2020-1154**		
Improper Privilege Management	21-05-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164. **CVE ID : CVE-2020-1155**	N/A	O-MIC-WIND-010620/767
Improper Privilege Management	21-05-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-	N/A	O-MIC-WIND-010620/768

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1158. **CVE ID : CVE-2020-1164**		
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when Windows improperly handles calls to Clipboard Service, aka 'Windows Clipboard Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1111, CVE-2020-1121, CVE-2020-1166. **CVE ID : CVE-2020-1165**	N/A	O-MIC-WIND-010620/769
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when Windows improperly handles calls to Clipboard Service, aka 'Windows Clipboard Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1111, CVE-2020-1121, CVE-2020-1165. **CVE ID : CVE-2020-1166**	N/A	O-MIC-WIND-010620/770
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1051, CVE-2020-1175, CVE-2020-1176. **CVE ID : CVE-2020-1174**	N/A	O-MIC-WIND-010620/771
Improper Restriction of Operations	21-05-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database	N/A	O-MIC-WIND-010620/772

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1051, CVE-2020-1174, CVE-2020-1176. **CVE ID : CVE-2020-1175**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1051, CVE-2020-1174, CVE-2020-1175. **CVE ID : CVE-2020-1176**	N/A	O-MIC-WIND-010620/773
Information Exposure	21-05-2020	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0963, CVE-2020-1141, CVE-2020-1145. **CVE ID : CVE-2020-1179**	N/A	O-MIC-WIND-010620/774
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows	N/A	O-MIC-WIND-010620/775

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1185, CVE-2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191. **CVE ID : CVE-2020-1184**		
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191. **CVE ID : CVE-2020-1185**	N/A	O-MIC-WIND-010620/776
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-	N/A	O-MIC-WIND-010620/777

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191. **CVE ID : CVE-2020-1186**		
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-2020-1186, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191. **CVE ID : CVE-2020-1187**	N/A	O-MIC-WIND-010620/778
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-2020-	N/A	O-MIC-WIND-010620/779

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1186, CVE-2020-1187, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191. **CVE ID : CVE-2020-1188**		
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1190, CVE-2020-1191. **CVE ID : CVE-2020-1189**	N/A	O-MIC-WIND-010620/780
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1191.	N/A	O-MIC-WIND-010620/781

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1190		
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190. **CVE ID : CVE-2020-1191**	N/A	O-MIC-WIND-010620/782
windows_server_2019					
Information Exposure	21-05-2020	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1141, CVE-2020-1145, CVE-2020-1179. **CVE ID : CVE-2020-0963**	N/A	O-MIC-WIND-010620/783
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system, aka 'Windows Print Spooler Elevation of	N/A	O-MIC-WIND-010620/784

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1070. **CVE ID : CVE-2020-1048**		
Improper Privilege Management	21-05-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164. **CVE ID : CVE-2020-1156**	N/A	O-MIC-WIND-010620/785
Improper Privilege Management	21-05-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1158, CVE-2020-1164. **CVE ID : CVE-2020-1157**	N/A	O-MIC-WIND-010620/786
Improper	21-05-2020	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 when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1164. **CVE ID : CVE-2020-1158**		010620/787
Improper Input Validation	21-05-2020	5	A denial of service vulnerability exists when Hyper-V on a Windows Server fails to properly handle specially crafted network packets.To exploit the vulnerability, an attacker would send specially crafted network packets to the Hyper-V Server.The security update addresses the vulnerability by resolving the conditions where Hyper-V would fail to properly handle these network packets., aka 'Windows Hyper-V Denial of Service Vulnerability'. **CVE ID : CVE-2020-0909**	N/A	O-MIC-WIND-010620/788
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists in Windows Block Level Backup Engine Service (wbengine) that allows file	N/A	O-MIC-WIND-010620/789

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			deletion in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1068, CVE-2020-1079. **CVE ID : CVE-2020-1010**		
Improper Privilege Management	21-05-2020	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-2020-1082, CVE-2020-1088. **CVE ID : CVE-2020-1021**	N/A	O-MIC-WIND-010620/790
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1126, CVE-2020-1136, CVE-2020-1150. **CVE ID : CVE-2020-1028**	N/A	O-MIC-WIND-010620/791
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution	N/A	O-MIC-WIND-010620/792

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. This CVE ID is unique from CVE-2020-1058, CVE-2020-1060, CVE-2020-1093. **CVE ID : CVE-2020-1035**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. **CVE ID : CVE-2020-1037**	N/A	O-MIC-WIND-010620/793
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1174, CVE-2020-1175, CVE-2020-1176. **CVE ID : CVE-2020-1051**	N/A	O-MIC-WIND-010620/794
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1143. **CVE ID : CVE-2020-1054**	N/A	O-MIC-WIND-010620/795

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-05-2020	4.3	A cross-site-scripting (XSS) vulnerability exists when Active Directory Federation Services (ADFS) does not properly sanitize user inputs, aka 'Microsoft Active Directory Federation Services Cross-Site Scripting Vulnerability'. **CVE ID : CVE-2020-1055**	N/A	O-MIC-WIND-010620/796
Incorrect Permission Assignment for Critical Resource	21-05-2020	5.8	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-2020-1056**	N/A	O-MIC-WIND-010620/797
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1035, CVE-2020-1060, CVE-2020-1093. **CVE ID : CVE-2020-1058**	N/A	O-MIC-WIND-010620/798
URL	21-05-2020	4.3	A spoofing vulnerability	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Redirection to Untrusted Site ('Open Redirect')			exists when Microsoft Edge does not properly parse HTTP content, aka 'Microsoft Edge Spoofing Vulnerability'. **CVE ID : CVE-2020-1059**		010620/799
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1035, CVE-2020-1058, CVE-2020-1093. **CVE ID : CVE-2020-1060**	N/A	O-MIC-WIND-010620/800
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists in the way that the Microsoft Script Runtime handles objects in memory, aka 'Microsoft Script Runtime Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1061**	N/A	O-MIC-WIND-010620/801
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1092. **CVE ID : CVE-2020-1062**	N/A	O-MIC-WIND-010620/802
Improper Input	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the MSHTML	N/A	O-MIC-WIND-010620/803

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			engine improperly validates input.An attacker could execute arbitrary code in the context of the current user, aka 'MSHTML Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1064**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	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'. **CVE ID : CVE-2020-1065**	N/A	O-MIC-WIND-010620/804
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	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-2020-1067**	N/A	O-MIC-WIND-010620/805
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists in Windows Media Service that allows file creation in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1010, CVE-2020-1079. **CVE ID : CVE-2020-1068**	N/A	O-MIC-WIND-010620/806
Improper Privilege	21-05-2020	7.2	An elevation of privilege vulnerability exists when	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			the Windows Print Spooler service improperly allows arbitrary writing to the file system, aka 'Windows Print Spooler Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1048. **CVE ID : CVE-2020-1070**		010620/807
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when Windows improperly handles errors tied to Remote Access Common Dialog, aka 'Windows Remote Access Common Dialog Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1071**	N/A	O-MIC-WIND-010620/808
Information Exposure	21-05-2020	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-2020-1072**	N/A	O-MIC-WIND-010620/809
Information Exposure	21-05-2020	2.1	An information disclosure vulnerability exists when Windows Subsystem for Linux improperly handles objects in memory, aka 'Windows Subsystem for Linux Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1075**	N/A	O-MIC-WIND-010620/810
Improper Restriction of Operations	21-05-2020	2.1	A denial of service vulnerability exists when Windows improperly	N/A	O-MIC-WIND-010620/811

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			handles objects in memory, aka 'Windows Denial of Service Vulnerability'. **CVE ID : CVE-2020-1076**		
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164. **CVE ID : CVE-2020-1077**	N/A	O-MIC-WIND-010620/812
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on the victim system, aka 'Windows Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1078**	N/A	O-MIC-WIND-010620/813
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Windows fails to properly handle objects in	N/A	O-MIC-WIND-010620/814

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1010, CVE-2020-1068. **CVE ID : CVE-2020-1079**		
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Windows Printer Service improperly validates file paths while loading printer drivers, aka 'Windows Printer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1081**	N/A	O-MIC-WIND-010620/815
Improper Privilege Management	21-05-2020	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-2020-1021, CVE-2020-1088. **CVE ID : CVE-2020-1082**	N/A	O-MIC-WIND-010620/816
Incorrect Permission Assignment for Critical Resource	21-05-2020	2.1	A Denial Of Service vulnerability exists when Connected User Experiences and Telemetry Service fails to validate certain function values.An attacker who successfully exploited this vulnerability could deny dependent security feature functionality.To exploit this	N/A	O-MIC-WIND-010620/817

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 Connected User Experiences and Telemetry Service validates certain function values., aka 'Connected User Experiences and Telemetry Service Denial of Service Vulnerability'. This CVE ID is unique from CVE-2020-1123. **CVE ID : CVE-2020-1084**		
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164. **CVE ID : CVE-2020-1086**	N/A	O-MIC-WIND-010620/818
Improper Privilege Management	21-05-2020	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-010620/819

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1114. **CVE ID : CVE-2020-1087**		
Improper Privilege Management	21-05-2020	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-2020-1021, CVE-2020-1082. **CVE ID : CVE-2020-1088**	N/A	O-MIC-WIND-010620/820
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164. **CVE ID : CVE-2020-1090**	N/A	O-MIC-WIND-010620/821
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory	N/A	O-MIC-WIND-010620/822

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1062. **CVE ID : CVE-2020-1092**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1035, CVE-2020-1058, CVE-2020-1060. **CVE ID : CVE-2020-1093**	N/A	O-MIC-WIND-010620/823
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	7.6	A remote code execution vulnerability exists when Microsoft Edge PDF Reader improperly handles objects in memory, aka 'Microsoft Edge PDF Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1096**	N/A	O-MIC-WIND-010620/824
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Windows Update Stack fails to properly handle objects in memory, aka 'Windows Update Stack Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1110. **CVE ID : CVE-2020-1109**	N/A	O-MIC-WIND-010620/825
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Windows Update Stack fails to properly handle objects in memory, aka	N/A	O-MIC-WIND-010620/826

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			'Windows Update Stack Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1109. **CVE ID : CVE-2020-1110**		
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when Windows improperly handles calls to Clipboard Service, aka 'Windows Clipboard Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1121, CVE-2020-1165, CVE-2020-1166. **CVE ID : CVE-2020-1111**	N/A	O-MIC-WIND-010620/827
Unrestricted Upload of File with Dangerous Type	21-05-2020	9	An elevation of privilege vulnerability exists when the Windows Background Intelligent Transfer Service (BITS) IIS module improperly handles uploaded content, aka 'Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1112**	N/A	O-MIC-WIND-010620/828
Improper Certificate Validation	21-05-2020	9.3	A security feature bypass vulnerability exists in Microsoft Windows when the Task Scheduler service fails to properly verify client connections over RPC, aka 'Windows Task Scheduler Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-1113**	N/A	O-MIC-WIND-010620/829

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	21-05-2020	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-2020-1087. **CVE ID : CVE-2020-1114**	N/A	O-MIC-WIND-010620/830
Information Exposure	21-05-2020	2.1	An information disclosure vulnerability exists when the Windows Client Server Run-Time Subsystem (CSRSS) fails to properly handle objects in memory, aka 'Windows CSRSS Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1116**	N/A	O-MIC-WIND-010620/831
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists in the way that the Color Management Module (ICM32.dll) handles objects in memory, aka 'Microsoft Color Management Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1117**	N/A	O-MIC-WIND-010620/832
N/A	21-05-2020	7.8	A denial of service vulnerability exists in the Windows implementation of Transport Layer Security (TLS) when it improperly handles certain key exchanges, aka 'Microsoft Windows Transport Layer Security Denial of Service	N/A	O-MIC-WIND-010620/833

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. **CVE ID : CVE-2020-1118**		
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when Windows improperly handles calls to Clipboard Service, aka 'Windows Clipboard Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1111, CVE-2020-1165, CVE-2020-1166. **CVE ID : CVE-2020-1121**	N/A	O-MIC-WIND-010620/834
Incorrect Permission Assignment for Critical Resource	21-05-2020	2.1	A denial of service vulnerability exists when Connected User Experiences and Telemetry Service improperly handles file operations, aka 'Connected User Experiences and Telemetry Service Denial of Service Vulnerability'. This CVE ID is unique from CVE-2020-1084. **CVE ID : CVE-2020-1123**	N/A	O-MIC-WIND-010620/835
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-	N/A	O-MIC-WIND-010620/836

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191. **CVE ID : CVE-2020-1124**		
Improper Privilege Management	21-05-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164. **CVE ID : CVE-2020-1125**	N/A	O-MIC-WIND-010620/837
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1028, CVE-2020-1136, CVE-2020-1150. **CVE ID : CVE-2020-1126**	N/A	O-MIC-WIND-010620/838
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows	N/A	O-MIC-WIND-010620/839

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191. **CVE ID : CVE-2020-1131**		
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles file and folder links, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1132**	N/A	O-MIC-WIND-010620/840
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191.	N/A	O-MIC-WIND-010620/841

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1134		
Improper Privilege Management	21-05-2020	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'. **CVE ID : CVE-2020-1135**	N/A	O-MIC-WIND-010620/842
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-1028, CVE-2020-1126, CVE-2020-1150. **CVE ID : CVE-2020-1136**	N/A	O-MIC-WIND-010620/843
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists in the way the Windows Push Notification Service handles objects in memory, aka 'Windows Push Notification Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1137**	N/A	O-MIC-WIND-010620/844
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when the Storage Service improperly handles file operations, aka 'Windows Storage Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1138**	N/A	O-MIC-WIND-010620/845

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	21-05-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164. **CVE ID : CVE-2020-1139**	N/A	O-MIC-WIND-010620/846
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1140**	N/A	O-MIC-WIND-010620/847
Information Exposure	21-05-2020	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'. This CVE ID is unique from CVE-2020-0963, CVE-2020-1145, CVE-2020-1179. **CVE ID : CVE-2020-1141**	N/A	O-MIC-WIND-010620/848

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, aka 'Windows GDI Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1142**	N/A	O-MIC-WIND-010620/849
Improper Privilege Management	21-05-2020	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1054. **CVE ID : CVE-2020-1143**	N/A	O-MIC-WIND-010620/850
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1184, CVE-2020-1185, CVE-2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191. **CVE ID : CVE-2020-1144**	N/A	O-MIC-WIND-010620/851
Improper	21-05-2020	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 when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164. **CVE ID : CVE-2020-1149**		010620/852
Improper Privilege Management	21-05-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164. **CVE ID : CVE-2020-1151**	N/A	O-MIC-WIND-010620/853
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Remote Code Execution	N/A	O-MIC-WIND-010620/854

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. **CVE ID : CVE-2020-1153**		
Improper Privilege Management	21-05-2020	7.2	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-2020-1154**	N/A	O-MIC-WIND-010620/855
Improper Privilege Management	21-05-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158, CVE-2020-1164. **CVE ID : CVE-2020-1155**	N/A	O-MIC-WIND-010620/856
Improper Privilege Management	21-05-2020	6.8	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1077, CVE-2020-1086, CVE-2020-1090, CVE-	N/A	O-MIC-WIND-010620/857

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-1125, CVE-2020-1139, CVE-2020-1149, CVE-2020-1151, CVE-2020-1155, CVE-2020-1156, CVE-2020-1157, CVE-2020-1158. **CVE ID : CVE-2020-1164**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1051, CVE-2020-1175, CVE-2020-1176. **CVE ID : CVE-2020-1174**	N/A	O-MIC-WIND-010620/858
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1051, CVE-2020-1174, CVE-2020-1176. **CVE ID : CVE-2020-1175**	N/A	O-MIC-WIND-010620/859
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-05-2020	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID	N/A	O-MIC-WIND-010620/860

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is unique from CVE-2020-1051, CVE-2020-1174, CVE-2020-1175. **CVE ID : CVE-2020-1176**		
Information Exposure	21-05-2020	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-0963, CVE-2020-1141, CVE-2020-1145. **CVE ID : CVE-2020-1179**	N/A	O-MIC-WIND-010620/861
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1185, CVE-2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191. **CVE ID : CVE-2020-1184**	N/A	O-MIC-WIND-010620/862
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects	N/A	O-MIC-WIND-010620/863

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191. **CVE ID : CVE-2020-1185**		
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191. **CVE ID : CVE-2020-1186**	N/A	O-MIC-WIND-010620/864
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID	N/A	O-MIC-WIND-010620/865

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-2020-1186, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191. **CVE ID : CVE-2020-1187**		
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-2020-1186, CVE-2020-1187, CVE-2020-1189, CVE-2020-1190, CVE-2020-1191. **CVE ID : CVE-2020-1188**	N/A	O-MIC-WIND-010620/866
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-	N/A	O-MIC-WIND-010620/867

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-1185, CVE-2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1190, CVE-2020-1191. **CVE ID : CVE-2020-1189**		
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1191. **CVE ID : CVE-2020-1190**	N/A	O-MIC-WIND-010620/868
Improper Privilege Management	21-05-2020	4.6	An elevation of privilege vulnerability exists when the Windows State Repository Service improperly handles objects in memory, aka 'Windows State Repository Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1124, CVE-2020-1131, CVE-2020-1134, CVE-2020-1144, CVE-2020-1184, CVE-2020-1185, CVE-2020-1186, CVE-2020-1187, CVE-2020-1188, CVE-2020-1189, CVE-2020-1190.	N/A	O-MIC-WIND-010620/869

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1191		
Netapp					
element_healthtools					
Information Exposure	21-05-2020	5	Element OS prior to version 12.0 and Element HealthTools prior to version 2020.04.01.04 are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information. **CVE ID : CVE-2020-8572**	N/A	O-NET-ELEM-010620/870
element_os					
Information Exposure	21-05-2020	5	Element OS prior to version 12.0 and Element HealthTools prior to version 2020.04.01.04 are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information. **CVE ID : CVE-2020-8572**	N/A	O-NET-ELEM-010620/871
Netgear					
r6220_firmware					
Improper Certificate Validation	28-05-2020	4.3	Certain NETGEAR devices are affected by Missing SSL Certificate Validation. This affects R7000 1.0.9.6_1.2.19 through 1.0.11.100_10.2.10, and possibly R6120, R7800, R6220, R8000, R6350, R9000, R6400, RAX120, R6400v2, RBR20, R6800, XR300, R6850, XR500, and R7000P.	N/A	O-NET-R622-010620/872

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-13245		
r6800_firmware					
Improper Certificate Validation	28-05-2020	4.3	Certain NETGEAR devices are affected by Missing SSL Certificate Validation. This affects R7000 1.0.9.6_1.2.19 through 1.0.11.100_10.2.10, and possibly R6120, R7800, R6220, R8000, R6350, R9000, R6400, RAX120, R6400v2, RBR20, R6800, XR300, R6850, XR500, and R7000P. **CVE ID : CVE-2020-13245**	N/A	O-NET-R680-010620/873
r6120_firmware					
Improper Certificate Validation	28-05-2020	4.3	Certain NETGEAR devices are affected by Missing SSL Certificate Validation. This affects R7000 1.0.9.6_1.2.19 through 1.0.11.100_10.2.10, and possibly R6120, R7800, R6220, R8000, R6350, R9000, R6400, RAX120, R6400v2, RBR20, R6800, XR300, R6850, XR500, and R7000P. **CVE ID : CVE-2020-13245**	N/A	O-NET-R612-010620/874
r6350_firmware					
Improper Certificate Validation	28-05-2020	4.3	Certain NETGEAR devices are affected by Missing SSL Certificate Validation. This affects R7000 1.0.9.6_1.2.19 through 1.0.11.100_10.2.10, and possibly R6120, R7800, R6220, R8000, R6350, R9000, R6400, RAX120, R6400v2, RBR20, R6800, XR300, R6850, XR500, and	N/A	O-NET-R635-010620/875

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R7000P. **CVE ID : CVE-2020-13245**		
r6850_firmware					
Improper Certificate Validation	28-05-2020	4.3	Certain NETGEAR devices are affected by Missing SSL Certificate Validation. This affects R7000 1.0.9.6_1.2.19 through 1.0.11.100_10.2.10, and possibly R6120, R7800, R6220, R8000, R6350, R9000, R6400, RAX120, R6400v2, RBR20, R6800, XR300, R6850, XR500, and R7000P. **CVE ID : CVE-2020-13245**	N/A	O-NET-R685-010620/876
xr300_firmware					
Improper Certificate Validation	28-05-2020	4.3	Certain NETGEAR devices are affected by Missing SSL Certificate Validation. This affects R7000 1.0.9.6_1.2.19 through 1.0.11.100_10.2.10, and possibly R6120, R7800, R6220, R8000, R6350, R9000, R6400, RAX120, R6400v2, RBR20, R6800, XR300, R6850, XR500, and R7000P. **CVE ID : CVE-2020-13245**	N/A	O-NET-XR30-010620/877
rbs50y_firmware					
Use of Hard-coded Credentials	18-05-2020	8.3	An issue was discovered on NETGEAR Orbi Tri-Band Business WiFi Add-on Satellite (SRS60) AC3000 V2.5.1.106, Outdoor Satellite (RBS50Y) V2.5.1.106, and Pro Tri-Band Business WiFi Router (SRR60) AC3000	N/A	O-NET-RBS5-010620/878

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V2.5.1.106. The root account has the same password as the Web-admin component. Thus, by exploiting CVE-2020-11551, it is possible to achieve remote code execution with root privileges on the embedded Linux system. **CVE ID : CVE-2020-11549**		
Information Exposure	18-05-2020	3.3	An issue was discovered on NETGEAR Orbi Tri-Band Business WiFi Add-on Satellite (SRS60) AC3000 V2.5.1.106, Outdoor Satellite (RBS50Y) V2.5.1.106, and Pro Tri-Band Business WiFi Router (SRR60) AC3000 V2.5.1.106. The administrative SOAP interface allows an unauthenticated remote leak of sensitive/arbitrary Wi-Fi information, such as SSIDs and Pre-Shared-Keys (PSK). **CVE ID : CVE-2020-11550**	N/A	O-NET-RBS5-010620/879
Improper Authentication	18-05-2020	5.8	An issue was discovered on NETGEAR Orbi Tri-Band Business WiFi Add-on Satellite (SRS60) AC3000 V2.5.1.106, Outdoor Satellite (RBS50Y) V2.5.1.106, and Pro Tri-Band Business WiFi Router (SRR60) AC3000 V2.5.1.106. The administrative SOAP interface allows an	N/A	O-NET-RBS5-010620/880

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated remote write of arbitrary Wi-Fi configuration data such as authentication details (e.g., the Web-admin password), network settings, DNS settings, system administration interface configuration, etc. **CVE ID : CVE-2020-11551**		
srr60_firmware					
Use of Hard-coded Credentials	18-05-2020	8.3	An issue was discovered on NETGEAR Orbi Tri-Band Business WiFi Add-on Satellite (SRS60) AC3000 V2.5.1.106, Outdoor Satellite (RBS50Y) V2.5.1.106, and Pro Tri-Band Business WiFi Router (SRR60) AC3000 V2.5.1.106. The root account has the same password as the Web-admin component. Thus, by exploiting CVE-2020-11551, it is possible to achieve remote code execution with root privileges on the embedded Linux system. **CVE ID : CVE-2020-11549**	N/A	O-NET-SRR6-010620/881
Information Exposure	18-05-2020	3.3	An issue was discovered on NETGEAR Orbi Tri-Band Business WiFi Add-on Satellite (SRS60) AC3000 V2.5.1.106, Outdoor Satellite (RBS50Y) V2.5.1.106, and Pro Tri-Band Business WiFi Router (SRR60) AC3000 V2.5.1.106. The	N/A	O-NET-SRR6-010620/882

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			administrative SOAP interface allows an unauthenticated remote leak of sensitive/arbitrary Wi-Fi information, such as SSIDs and Pre-Shared-Keys (PSK). **CVE ID : CVE-2020-11550**		
Improper Authentication	18-05-2020	5.8	An issue was discovered on NETGEAR Orbi Tri-Band Business WiFi Add-on Satellite (SRS60) AC3000 V2.5.1.106, Outdoor Satellite (RBS50Y) V2.5.1.106, and Pro Tri-Band Business WiFi Router (SRR60) AC3000 V2.5.1.106. The administrative SOAP interface allows an unauthenticated remote write of arbitrary Wi-Fi configuration data such as authentication details (e.g., the Web-admin password), network settings, DNS settings, system administration interface configuration, etc. **CVE ID : CVE-2020-11551**	N/A	O-NET-SRR6-010620/883
srs60_firmware					
Use of Hard-coded Credentials	18-05-2020	8.3	An issue was discovered on NETGEAR Orbi Tri-Band Business WiFi Add-on Satellite (SRS60) AC3000 V2.5.1.106, Outdoor Satellite (RBS50Y) V2.5.1.106, and Pro Tri-Band Business WiFi Router (SRR60) AC3000	N/A	O-NET-SRS6-010620/884

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V2.5.1.106. The root account has the same password as the Web-admin component. Thus, by exploiting CVE-2020-11551, it is possible to achieve remote code execution with root privileges on the embedded Linux system. **CVE ID : CVE-2020-11549**		
Information Exposure	18-05-2020	3.3	An issue was discovered on NETGEAR Orbi Tri-Band Business WiFi Add-on Satellite (SRS60) AC3000 V2.5.1.106, Outdoor Satellite (RBS50Y) V2.5.1.106, and Pro Tri-Band Business WiFi Router (SRR60) AC3000 V2.5.1.106. The administrative SOAP interface allows an unauthenticated remote leak of sensitive/arbitrary Wi-Fi information, such as SSIDs and Pre-Shared-Keys (PSK). **CVE ID : CVE-2020-11550**	N/A	O-NET-SRS6-010620/885
Improper Authentication	18-05-2020	5.8	An issue was discovered on NETGEAR Orbi Tri-Band Business WiFi Add-on Satellite (SRS60) AC3000 V2.5.1.106, Outdoor Satellite (RBS50Y) V2.5.1.106, and Pro Tri-Band Business WiFi Router (SRR60) AC3000 V2.5.1.106. The administrative SOAP interface allows an	N/A	O-NET-SRS6-010620/886

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated remote write of arbitrary Wi-Fi configuration data such as authentication details (e.g., the Web-admin password), network settings, DNS settings, system administration interface configuration, etc. **CVE ID : CVE-2020-11551**		
r8000_firmware					
Improper Certificate Validation	28-05-2020	4.3	Certain NETGEAR devices are affected by Missing SSL Certificate Validation. This affects R7000 1.0.9.6_1.2.19 through 1.0.11.100_10.2.10, and possibly R6120, R7800, R6220, R8000, R6350, R9000, R6400, RAX120, R6400v2, RBR20, R6800, XR300, R6850, XR500, and R7000P. **CVE ID : CVE-2020-13245**	N/A	O-NET-R800-010620/887
r6400_firmware					
Improper Certificate Validation	28-05-2020	4.3	Certain NETGEAR devices are affected by Missing SSL Certificate Validation. This affects R7000 1.0.9.6_1.2.19 through 1.0.11.100_10.2.10, and possibly R6120, R7800, R6220, R8000, R6350, R9000, R6400, RAX120, R6400v2, RBR20, R6800, XR300, R6850, XR500, and R7000P. **CVE ID : CVE-2020-13245**	N/A	O-NET-R640-010620/888
r7000p_firmware					
Improper	28-05-2020	4.3	Certain NETGEAR devices	N/A	O-NET-R700-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Certificate Validation			are affected by Missing SSL Certificate Validation. This affects R7000 1.0.9.6_1.2.19 through 1.0.11.100_10.2.10, and possibly R6120, R7800, R6220, R8000, R6350, R9000, R6400, RAX120, R6400v2, RBR20, R6800, XR300, R6850, XR500, and R7000P. **CVE ID : CVE-2020-13245**		010620/889
r7800_firmware					
Improper Certificate Validation	28-05-2020	4.3	Certain NETGEAR devices are affected by Missing SSL Certificate Validation. This affects R7000 1.0.9.6_1.2.19 through 1.0.11.100_10.2.10, and possibly R6120, R7800, R6220, R8000, R6350, R9000, R6400, RAX120, R6400v2, RBR20, R6800, XR300, R6850, XR500, and R7000P. **CVE ID : CVE-2020-13245**	N/A	O-NET-R780-010620/890
r9000_firmware					
Improper Certificate Validation	28-05-2020	4.3	Certain NETGEAR devices are affected by Missing SSL Certificate Validation. This affects R7000 1.0.9.6_1.2.19 through 1.0.11.100_10.2.10, and possibly R6120, R7800, R6220, R8000, R6350, R9000, R6400, RAX120, R6400v2, RBR20, R6800, XR300, R6850, XR500, and R7000P. **CVE ID : CVE-2020-13245**	N/A	O-NET-R900-010620/891
rax120_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Certificate Validation	28-05-2020	4.3	Certain NETGEAR devices are affected by Missing SSL Certificate Validation. This affects R7000 1.0.9.6_1.2.19 through 1.0.11.100_10.2.10, and possibly R6120, R7800, R6220, R8000, R6350, R9000, R6400, RAX120, R6400v2, RBR20, R6800, XR300, R6850, XR500, and R7000P. **CVE ID : CVE-2020-13245**	N/A	O-NET-RAX1-010620/892
xr500_firmware					
Improper Certificate Validation	28-05-2020	4.3	Certain NETGEAR devices are affected by Missing SSL Certificate Validation. This affects R7000 1.0.9.6_1.2.19 through 1.0.11.100_10.2.10, and possibly R6120, R7800, R6220, R8000, R6350, R9000, R6400, RAX120, R6400v2, RBR20, R6800, XR300, R6850, XR500, and R7000P. **CVE ID : CVE-2020-13245**	N/A	O-NET-XR50-010620/893
rbr20_firmware					
Improper Certificate Validation	28-05-2020	4.3	Certain NETGEAR devices are affected by Missing SSL Certificate Validation. This affects R7000 1.0.9.6_1.2.19 through 1.0.11.100_10.2.10, and possibly R6120, R7800, R6220, R8000, R6350, R9000, R6400, RAX120, R6400v2, RBR20, R6800, XR300, R6850, XR500, and R7000P. **CVE ID : CVE-2020-13245**	N/A	O-NET-RBR2-010620/894

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Panasonic					
p99_firmware					
N/A	19-05-2020	7.5	Panasonic P99 devices through 2020-04-10 have Incorrect Access Control. NOTE: the vendor states that all affected products are at "End-of-software-support." **CVE ID : CVE-2020-11715**	https://mobile.panasonic.com/in/advisory	O-PAN-P99_-010620/895
p110_firmware					
Incorrect Default Permissions	20-05-2020	7.5	Panasonic P110, Eluga Z1 Pro, Eluga X1, and Eluga X1 Pro devices through 2020-04-10 have Insecure Permissions. NOTE: the vendor states that all affected products are at "End-of-software-support." **CVE ID : CVE-2020-11716**	https://mobile.panasonic.com/in/advisory	O-PAN-P110-010620/896
eluga_z1_pro_firmware					
Incorrect Default Permissions	20-05-2020	7.5	Panasonic P110, Eluga Z1 Pro, Eluga X1, and Eluga X1 Pro devices through 2020-04-10 have Insecure Permissions. NOTE: the vendor states that all affected products are at "End-of-software-support." **CVE ID : CVE-2020-11716**	https://mobile.panasonic.com/in/advisory	O-PAN-ELUG-010620/897
eluga_x1_firmware					
Incorrect Default Permissions	20-05-2020	7.5	Panasonic P110, Eluga Z1 Pro, Eluga X1, and Eluga X1 Pro devices through 2020-04-10 have Insecure Permissions. NOTE: the vendor states that all affected products are at	https://mobile.panasonic.com/in/advisory	O-PAN-ELUG-010620/898

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"End-of-software-support." **CVE ID : CVE-2020-11716**		
eluga_x1_pro_firmware					
Incorrect Default Permissions	20-05-2020	7.5	Panasonic P110, Eluga Z1 Pro, Eluga X1, and Eluga X1 Pro devices through 2020-04-10 have Insecure Permissions. NOTE: the vendor states that all affected products are at "End-of-software-support." **CVE ID : CVE-2020-11716**	https://mobile.panasonic.com/in/advisory	O-PAN-ELUG-010620/899
eluga_ray_530_firmware					
Incorrect Default Permissions	20-05-2020	7.5	Panasonic P110, Eluga Z1 Pro, Eluga X1, and Eluga X1 Pro devices through 2020-04-10 have Insecure Permissions. NOTE: the vendor states that all affected products are at "End-of-software-support." **CVE ID : CVE-2020-11716**	https://mobile.panasonic.com/in/advisory	O-PAN-ELUG-010620/900
eluga_ray_600_firmware					
Incorrect Default Permissions	20-05-2020	7.5	Panasonic P110, Eluga Z1 Pro, Eluga X1, and Eluga X1 Pro devices through 2020-04-10 have Insecure Permissions. NOTE: the vendor states that all affected products are at "End-of-software-support." **CVE ID : CVE-2020-11716**	https://mobile.panasonic.com/in/advisory	O-PAN-ELUG-010620/901
Redhat					
enterprise_linux_aus					
NULL Pointer Dereference	22-05-2020	5	A NULL pointer dereference flaw was found in the Linux kernel's SELinux subsystem	https://bugzilla.redhat.com	O-RED-ENTE-010620/902

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in versions before 5.7. This flaw occurs while importing the Commercial IP Security Option (CIPSO) protocol's category bitmap into the SELinux extensible bitmap via the' ebitmap_netlbl_import' routine. While processing the CIPSO restricted bitmap tag in the 'cipso_v4_parsetag_rbm' routine, it sets the security attribute to indicate that the category bitmap is present, even if it has not been allocated. This issue leads to a NULL pointer dereference issue while importing the same category bitmap into SELinux. This flaw allows a remote network user to crash the system kernel, resulting in a denial of service. **CVE ID : CVE-2020-10711**	/show_bug.cgi?id=CVE-2020-10711, https://www.openwall.com/lists/oss-security/2020/05/12/2	
messaging_realtime_grid					
NULL Pointer Dereference	22-05-2020	5	A NULL pointer dereference flaw was found in the Linux kernel's SELinux subsystem in versions before 5.7. This flaw occurs while importing the Commercial IP Security Option (CIPSO) protocol's category bitmap into the SELinux extensible bitmap via the' ebitmap_netlbl_import' routine. While processing the CIPSO restricted bitmap	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10711, https://www.openwall.com/lists/oss-security/2020/05/	O-RED-MESS-010620/903

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			tag in the 'cipso_v4_parsetag_rbm' routine, it sets the security attribute to indicate that the category bitmap is present, even if it has not been allocated. This issue leads to a NULL pointer dereference issue while importing the same category bitmap into SELinux. This flaw allows a remote network user to crash the system kernel, resulting in a denial of service. **CVE ID : CVE-2020-10711**	12/2	
enterprise_linux_server_tus					
NULL Pointer Dereference	22-05-2020	5	A NULL pointer dereference flaw was found in the Linux kernel's SELinux subsystem in versions before 5.7. This flaw occurs while importing the Commercial IP Security Option (CIPSO) protocol's category bitmap into the SELinux extensible bitmap via the' ebitmap_netlbl_import' routine. While processing the CIPSO restricted bitmap tag in the 'cipso_v4_parsetag_rbm' routine, it sets the security attribute to indicate that the category bitmap is present, even if it has not been allocated. This issue leads to a NULL pointer dereference issue while importing the same category bitmap into	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10711, https://www.openwall.com/lists/oss-security/2020/05/12/2	O-RED-ENTE-010620/904

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SELinux. This flaw allows a remote network user to crash the system kernel, resulting in a denial of service. **CVE ID : CVE-2020-10711**		
enterprise_linux					
NULL Pointer Dereference	22-05-2020	5	A NULL pointer dereference flaw was found in the Linux kernel's SELinux subsystem in versions before 5.7. This flaw occurs while importing the Commercial IP Security Option (CIPSO) protocol's category bitmap into the SELinux extensible bitmap via the' ebitmap_netlbl_import' routine. While processing the CIPSO restricted bitmap tag in the 'cipso_v4_parsetag_rbm' routine, it sets the security attribute to indicate that the category bitmap is present, even if it has not been allocated. This issue leads to a NULL pointer dereference issue while importing the same category bitmap into SELinux. This flaw allows a remote network user to crash the system kernel, resulting in a denial of service. **CVE ID : CVE-2020-10711**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10711, https://www.openwall.com/lists/oss-security/2020/05/12/2	O-RED-ENTE-010620/905
Tendacn					
ac6_firmware					
Buffer Copy	22-05-2020	7.5	An issue was discovered on	N/A	O-TEN-AC6_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/SetNetControlList list parameter for a POST request, a value is directly used in a strcpy to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13394**		010620/906
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the	N/A	O-TEN-AC6_-010620/907

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			/goform/openSchedWifi schedStartTime and schedEndTime parameters for a POST request, a value is directly used in a strcpy to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13389**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/addressNat entrys and mitInterface parameters for a POST request, a value is directly used in a sprintf to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks.	N/A	O-TEN-AC6_-010620/908

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-13390		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/SetSpeedWan speed_dir parameter for a POST request, a value is directly used in a sprintf to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13391**	N/A	O-TEN-AC6_-010620/909
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer	N/A	O-TEN-AC6_-010620/910

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			overflow vulnerability in the router's web server -- httpd. While processing the /goform/setcfm funcpara1 parameter for a POST request, a value is directly used in a sprintf to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13392**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/saveParentControlInfo deviceId and time parameters for a POST request, a value is directly used in a strcpy to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution	N/A	O-TEN-AC6_-010620/911

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks. **CVE ID : CVE-2020-13393**		
ac9_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/SetNetControlList list parameter for a POST request, a value is directly used in a strcpy to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13394**	N/A	O-TEN-AC9_-010620/912
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18	N/A	O-TEN-AC9_-010620/913

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/openSchedWifi schedStartTime and schedEndTime parameters for a POST request, a value is directly used in a strcpy to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13389**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/addressNat entrys and mitInterface parameters for a POST request, a value is directly used in a sprintf to a local variable placed on the stack, which overwrites the return address of a function. An	N/A	O-TEN-AC9_-010620/914

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13390**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/SetSpeedWan speed_dir parameter for a POST request, a value is directly used in a sprintf to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13391**	N/A	O-TEN-AC9_-010620/915
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0	N/A	O-TEN-AC9_-010620/916

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/setcfm funcpara1 parameter for a POST request, a value is directly used in a sprintf to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13392**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/saveParentControlInfo deviceId and time parameters for a POST request, a value is directly used in a strcpy to a local variable placed on the stack, which overwrites the return	N/A	O-TEN-AC9_-010620/917

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13393**		
ac15_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/SetNetControlList list parameter for a POST request, a value is directly used in a strcpy to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13394**	N/A	O-TEN-AC15-010620/918
Buffer Copy without Checking Size of Input ('Classic Buffer	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0	N/A	O-TEN-AC15-010620/919

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/openSchedWifi schedStartTime and schedEndTime parameters for a POST request, a value is directly used in a strcpy to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13389**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/addressNat entrys and mitInterface parameters for a POST request, a value is directly	N/A	O-TEN-AC15-010620/920

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			used in a sprintf to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13390**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/SetSpeedWan speed_dir parameter for a POST request, a value is directly used in a sprintf to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13391**	N/A	O-TEN-AC15-010620/921
Buffer Copy without Checking Size of Input	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0	N/A	O-TEN-AC15-010620/922

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/setcfm funcpara1 parameter for a POST request, a value is directly used in a sprintf to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13392**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/saveParentControl Info deviceId and time parameters for a POST	N/A	O-TEN-AC15-010620/923

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request, a value is directly used in a strcpy to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13393**		
ac18_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/SetNetControlList list parameter for a POST request, a value is directly used in a strcpy to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13394**	N/A	O-TEN-AC18-010620/924
Buffer Copy without	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0	N/A	O-TEN-AC18-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/openSchedWifi schedStartTime and schedEndTime parameters for a POST request, a value is directly used in a strcpy to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13389**		010620/925
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the	N/A	O-TEN-AC18-010620/926

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			/goform/addressNat entrys and mitInterface parameters for a POST request, a value is directly used in a sprintf to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13390**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/SetSpeedWan speed_dir parameter for a POST request, a value is directly used in a sprintf to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13391**	N/A	O-TEN-AC18-010620/927

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/setcfm funcpara1 parameter for a POST request, a value is directly used in a sprintf to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13392**	N/A	O-TEN-AC18-010620/928
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server --	N/A	O-TEN-AC18-010620/929

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			httpd. While processing the /goform/saveParentControlInfo deviceId and time parameters for a POST request, a value is directly used in a strcpy to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13393**		
thetrackr					
trackr_firmware					
Missing Authorization	23-05-2020	6.8	TrackR devices through 2020-05-06 allow attackers to trigger the Beep (aka alarm) feature, which will eventually cause a denial of service when battery capacity is exhausted. **CVE ID : CVE-2020-13425**	N/A	O-THE-TRAC-010620/930
ui					
airos					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users	N/A	O-UI-AIRO-010620/931

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**	N/A	O-UI-AIRO-010620/932
Improper Neutralization of Special	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for	N/A	O-UI-AIRO-010620/933

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**		
Vmware					
photon_os					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-05-2020	6.5	VMware Cloud Director 10.0.x before 10.0.0.2, 9.7.0.x before 9.7.0.5, 9.5.0.x before 9.5.0.6, and 9.1.0.x before 9.1.0.4 do not properly handle input leading to a code injection vulnerability. An authenticated actor may be able to send malicious traffic to VMware Cloud Director which may lead to arbitrary remote code execution. This vulnerability can be exploited through the HTML5- and Flex-based UIs, the API Explorer interface	N/A	O-VMW-PHOT-010620/934

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and API access. **CVE ID : CVE-2020-3956**		
Hardware					
bosch					
recording_station					
Exposure of Resource to Wrong Sphere	27-05-2020	7.2	Improper Access Control in the Kiosk Mode functionality of Bosch Recording Station allows a local unauthenticated attacker to escape from the Kiosk Mode and access the underlying operating system. **CVE ID : CVE-2020-6774**	N/A	H-BOS-RECO-010620/935
Dell					
dock_wd15					
Uncontrolled Search Path Element	28-05-2020	2.6	Dell Dock Firmware Update Utilities for Dell Client Consumer and Commercial docking stations contain an Arbitrary File Overwrite vulnerability. The vulnerability is limited to the Dell Dock Firmware Update Utilities during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect	N/A	H-DEL-DOCK-010620/936

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the actual binary payload that the update utility delivers. **CVE ID : CVE-2020-5357**		
dock_wd19					
Uncontrolled Search Path Element	28-05-2020	2.6	Dell Dock Firmware Update Utilities for Dell Client Consumer and Commercial docking stations contain an Arbitrary File Overwrite vulnerability. The vulnerability is limited to the Dell Dock Firmware Update Utilities during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. **CVE ID : CVE-2020-5357**	N/A	H-DEL-DOCK-010620/937
thunderbolt_dock_tb16					
Uncontrolled Search Path Element	28-05-2020	2.6	Dell Dock Firmware Update Utilities for Dell Client Consumer and Commercial docking stations contain an Arbitrary File Overwrite vulnerability. The vulnerability is limited to the Dell Dock Firmware	N/A	H-DEL-THUN-010620/938

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Update Utilities during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload that the update utility delivers. **CVE ID : CVE-2020-5357**		
precision_dual_usb-c_thunderbolt_dock_-_tb18dc					
Uncontrolled Search Path Element	28-05-2020	2.6	Dell Dock Firmware Update Utilities for Dell Client Consumer and Commercial docking stations contain an Arbitrary File Overwrite vulnerability. The vulnerability is limited to the Dell Dock Firmware Update Utilities during the time window while being executed by an administrator. During this time window, a locally authenticated low-privileged malicious user could exploit this vulnerability by tricking an administrator into overwriting arbitrary files via a symlink attack. The vulnerability does not affect the actual binary payload	N/A	H-DEL-PREC-010620/939

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that the update utility delivers. **CVE ID : CVE-2020-5357**		
D-link					
dsp-w215					
Information Exposure	18-05-2020	3.3	D-Link DSP-W215 1.26b03 devices allow information disclosure by intercepting messages on the local network, as demonstrated by a Squid Proxy. **CVE ID : CVE-2020-13135**	N/A	H-D-L-DSP--010620/940
Information Exposure	18-05-2020	5	D-Link DSP-W215 1.26b03 devices send an obfuscated hash that can be retrieved and understood by a network sniffer. **CVE ID : CVE-2020-13136**	N/A	H-D-L-DSP--010620/941
Epson					
eb-1470ui					
Information Exposure	22-05-2020	6.4	An exploitable authentication bypass vulnerability exists in the ESPON Web Control functionality of Epson EB-1470Ui MAIN: 98009273ESWWV107 MAIN2: 8X7325WWV303. A specially crafted series of HTTP requests can cause authentication bypass resulting in information disclosure. An attacker can send an HTTP request to trigger this vulnerability. **CVE ID : CVE-2020-6091**	N/A	H-EPS-EB-1-010620/942
hpe					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
nimble_storage_af20_all_flash_array					
Improper Input Validation	19-05-2020	6.5	Potential remote code execution security vulnerabilities have been identified with HPE Nimble Storage systems that could be exploited by an attacker to gain elevated privileges on the array. The following NimbleOS versions, and all subsequent releases, contain a software fix for this vulnerability: 3.9.3.0 4.5.6.0 5.0.9.0 5.1.4.100 **CVE ID : CVE-2020-7138**	N/A	H-HPE-NIMB-010620/943
Information Exposure	19-05-2020	5.5	Potential remote access security vulnerabilities have been identified with HPE Nimble Storage systems that could be exploited by an attacker to access and modify sensitive information on the system. The following NimbleOS versions, and all subsequent releases, contain a software fix for this vulnerability: 3.9.3.0 4.5.6.0 5.0.9.0 5.1.4.100 **CVE ID : CVE-2020-7139**	N/A	H-HPE-NIMB-010620/944
nimble_storage_af20q_all_flash_dual_controller					
Improper Input Validation	19-05-2020	6.5	Potential remote code execution security vulnerabilities have been identified with HPE Nimble Storage systems that could be exploited by an attacker to gain elevated privileges on the array. The following	N/A	H-HPE-NIMB-010620/945

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NimbleOS versions, and all subsequent releases, contain a software fix for this vulnerability: 3.9.3.0 4.5.6.0 5.0.9.0 5.1.4.100 **CVE ID : CVE-2020-7138**		
Information Exposure	19-05-2020	5.5	Potential remote access security vulnerabilities have been identified with HPE Nimble Storage systems that could be exploited by an attacker to access and modify sensitive information on the system. The following NimbleOS versions, and all subsequent releases, contain a software fix for this vulnerability: 3.9.3.0 4.5.6.0 5.0.9.0 5.1.4.100 **CVE ID : CVE-2020-7139**	N/A	H-HPE-NIMB-010620/946
nimble_storage_af40_all_flash_dual_controller					
Improper Input Validation	19-05-2020	6.5	Potential remote code execution security vulnerabilities have been identified with HPE Nimble Storage systems that could be exploited by an attacker to gain elevated privileges on the array. The following NimbleOS versions, and all subsequent releases, contain a software fix for this vulnerability: 3.9.3.0 4.5.6.0 5.0.9.0 5.1.4.100 **CVE ID : CVE-2020-7138**	N/A	H-HPE-NIMB-010620/947
Information Exposure	19-05-2020	5.5	Potential remote access security vulnerabilities have been identified with	N/A	H-HPE-NIMB-010620/948

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HPE Nimble Storage systems that could be exploited by an attacker to access and modify sensitive information on the system. The following NimbleOS versions, and all subsequent releases, contain a software fix for this vulnerability: 3.9.3.0 4.5.6.0 5.0.9.0 5.1.4.100 **CVE ID : CVE-2020-7139**		
nimble_storage_af60_all_flash_dual_controller					
Improper Input Validation	19-05-2020	6.5	Potential remote code execution security vulnerabilities have been identified with HPE Nimble Storage systems that could be exploited by an attacker to gain elevated privileges on the array. The following NimbleOS versions, and all subsequent releases, contain a software fix for this vulnerability: 3.9.3.0 4.5.6.0 5.0.9.0 5.1.4.100 **CVE ID : CVE-2020-7138**	N/A	H-HPE-NIMB-010620/949
Information Exposure	19-05-2020	5.5	Potential remote access security vulnerabilities have been identified with HPE Nimble Storage systems that could be exploited by an attacker to access and modify sensitive information on the system. The following NimbleOS versions, and all subsequent releases, contain a software fix for this vulnerability: 3.9.3.0 4.5.6.0 5.0.9.0	N/A	H-HPE-NIMB-010620/950

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			5.1.4.100 **CVE ID : CVE-2020-7139**		
nimble_storage_af80_all_flash_dual_controller					
Improper Input Validation	19-05-2020	6.5	Potential remote code execution security vulnerabilities have been identified with HPE Nimble Storage systems that could be exploited by an attacker to gain elevated privileges on the array. The following NimbleOS versions, and all subsequent releases, contain a software fix for this vulnerability: 3.9.3.0 4.5.6.0 5.0.9.0 5.1.4.100 **CVE ID : CVE-2020-7138**	N/A	H-HPE-NIMB-010620/951
Information Exposure	19-05-2020	5.5	Potential remote access security vulnerabilities have been identified with HPE Nimble Storage systems that could be exploited by an attacker to access and modify sensitive information on the system. The following NimbleOS versions, and all subsequent releases, contain a software fix for this vulnerability: 3.9.3.0 4.5.6.0 5.0.9.0 5.1.4.100 **CVE ID : CVE-2020-7139**	N/A	H-HPE-NIMB-010620/952
nimble_storage_cs3000					
Improper Input Validation	19-05-2020	6.5	Potential remote code execution security vulnerabilities have been identified with HPE Nimble Storage systems that could be exploited by an attacker	N/A	H-HPE-NIMB-010620/953

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to gain elevated privileges on the array. The following NimbleOS versions, and all subsequent releases, contain a software fix for this vulnerability: 3.9.3.0 4.5.6.0 5.0.9.0 5.1.4.100 **CVE ID : CVE-2020-7138**		
Information Exposure	19-05-2020	5.5	Potential remote access security vulnerabilities have been identified with HPE Nimble Storage systems that could be exploited by an attacker to access and modify sensitive information on the system. The following NimbleOS versions, and all subsequent releases, contain a software fix for this vulnerability: 3.9.3.0 4.5.6.0 5.0.9.0 5.1.4.100 **CVE ID : CVE-2020-7139**	N/A	H-HPE-NIMB-010620/954
nimble_storage_cs5000					
Improper Input Validation	19-05-2020	6.5	Potential remote code execution security vulnerabilities have been identified with HPE Nimble Storage systems that could be exploited by an attacker to gain elevated privileges on the array. The following NimbleOS versions, and all subsequent releases, contain a software fix for this vulnerability: 3.9.3.0 4.5.6.0 5.0.9.0 5.1.4.100 **CVE ID : CVE-2020-7138**	N/A	H-HPE-NIMB-010620/955
Information	19-05-2020	5.5	Potential remote access	N/A	H-HPE-NIMB-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			security vulnerabilities have been identified with HPE Nimble Storage systems that could be exploited by an attacker to access and modify sensitive information on the system. The following NimbleOS versions, and all subsequent releases, contain a software fix for this vulnerability: 3.9.3.0 4.5.6.0 5.0.9.0 5.1.4.100 **CVE ID : CVE-2020-7139**		010620/956
nimble_storage_cs7000					
Improper Input Validation	19-05-2020	6.5	Potential remote code execution security vulnerabilities have been identified with HPE Nimble Storage systems that could be exploited by an attacker to gain elevated privileges on the array. The following NimbleOS versions, and all subsequent releases, contain a software fix for this vulnerability: 3.9.3.0 4.5.6.0 5.0.9.0 5.1.4.100 **CVE ID : CVE-2020-7138**	N/A	H-HPE-NIMB-010620/957
Information Exposure	19-05-2020	5.5	Potential remote access security vulnerabilities have been identified with HPE Nimble Storage systems that could be exploited by an attacker to access and modify sensitive information on the system. The following NimbleOS versions, and all subsequent releases, contain a software	N/A	H-HPE-NIMB-010620/958

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			fix for this vulnerability: 3.9.3.0 4.5.6.0 5.0.9.0 5.1.4.100 **CVE ID : CVE-2020-7139**		
nimble_storage_secondary_flash_arrays					
Improper Input Validation	19-05-2020	6.5	Potential remote code execution security vulnerabilities have been identified with HPE Nimble Storage systems that could be exploited by an attacker to gain elevated privileges on the array. The following NimbleOS versions, and all subsequent releases, contain a software fix for this vulnerability: 3.9.3.0 4.5.6.0 5.0.9.0 5.1.4.100 **CVE ID : CVE-2020-7138**	N/A	H-HPE-NIMB-010620/959
Information Exposure	19-05-2020	5.5	Potential remote access security vulnerabilities have been identified with HPE Nimble Storage systems that could be exploited by an attacker to access and modify sensitive information on the system. The following NimbleOS versions, and all subsequent releases, contain a software fix for this vulnerability: 3.9.3.0 4.5.6.0 5.0.9.0 5.1.4.100 **CVE ID : CVE-2020-7139**	N/A	H-HPE-NIMB-010620/960
superdome_flex_server					
Improper Input Validation	19-05-2020	4.6	A validation issue in HPE Superdome Flex's RMC component may allow local elevation of privilege. Apply	N/A	H-HPE-SUPE-010620/961

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HPE Superdome Flex Server version 3.25.46 or later to resolve this issue. **CVE ID : CVE-2020-7137**		
Huawei					
e6878-370					
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in some Huawei products. An unauthenticated, adjacent attacker could exploit this vulnerability to decrypt data. Successful exploitation may leak information randomly. Affected product versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions	N/A	H-HUA-E687-010620/962

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than 9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00AY Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00BX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		
Use After Free	21-05-2020	5.4	E6878-370 with versions of 10.0.3.1(H557SP27C233), 10.0.3.1(H563SP1C00), 10.0.3.1(H563SP1C233) has a use after free vulnerability. The software references memory after it has been freed in certain scenario, the attacker does a series of crafted operations through web portal, successful exploit could cause a use after free condition which may lead to malicious code execution. **CVE ID : CVE-2020-1799**	N/A	H-HUA-E687-010620/963
anne-al00					
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in some Huawei products. An unauthenticated, adjacent attacker could exploit this vulnerability to decrypt data. Successful exploitation may leak information randomly. Affected product versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions	N/A	H-HUA-ANNE-010620/964

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than 9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00AY Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00BX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1);		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		
berkeley-l09					
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in some Huawei products. An unauthenticated, adjacent attacker could exploit this vulnerability to decrypt data. Successful exploitation may leak information randomly. Affected product versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than	N/A	H-HUA-BERK-010620/965

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than 9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00AY Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00BX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1), Versions earlier than		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		
cd17-16					
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in some Huawei products. An unauthenticated, adjacent attacker could exploit this vulnerability to decrypt data. Successful exploitation may leak information randomly. Affected product versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10	N/A	H-HUA-CD17-010620/966

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than 9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00AY Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00BX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1),		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		
cd18-16					
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in some Huawei products. An unauthenticated, adjacent attacker could exploit this vulnerability to decrypt data. Successful exploitation may leak information randomly. Affected product versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than	N/A	H-HUA-CD18-010620/967

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than 9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00AY Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00BX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		
columbia-tl00b					
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in some Huawei products. An unauthenticated, adjacent attacker could exploit this vulnerability to decrypt data. Successful exploitation may leak information randomly. Affected product versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions	N/A	H-HUA-COLU-010620/968

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than 9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00AY Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00BX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier than 10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		
lelandp-l22a					
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in some Huawei products. An unauthenticated, adjacent attacker could exploit this vulnerability to decrypt data. Successful exploitation may leak information randomly. Affected product versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8);	N/A	H-HUA-LELA-010620/969

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than 9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00AY Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00BX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1);		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		
tc5200-16					
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in some Huawei products. An unauthenticated, adjacent attacker could exploit this vulnerability to decrypt data. Successful exploitation may leak information randomly. Affected product versions include: Anne-AL00 Versions earlier than	N/A	H-HUA-TC52-010620/970

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than 9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00AY Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00BX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		
ws5200-16					
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in some Huawei products. An unauthenticated, adjacent attacker could exploit this vulnerability to decrypt data. Successful exploitation may leak information randomly. Affected product versions include: Anne-	N/A	H-HUA-WS52-010620/971

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than 9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00AY Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00BX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-L03BX Versions		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		
ws5200-17					
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in some Huawei products. An unauthenticated, adjacent attacker could exploit this vulnerability to decrypt data. Successful exploitation may leak information randomly. Affected product	N/A	H-HUA-WS52-010620/972

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than 9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00AY Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00BX Versions earlier than 10.0.0.158(C00E64R1P9);		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		
ws5800-10					
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in some Huawei products. An unauthenticated, adjacent attacker could exploit this vulnerability to decrypt data. Successful exploitation may leak information	N/A	H-HUA-WS58-010620/973

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			randomly. Affected product versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than 9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00AY Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00BX Versions earlier than		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		
ws6500-16					
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in some Huawei products. An unauthenticated, adjacent attacker could exploit this vulnerability to decrypt data. Successful exploitation	N/A	H-HUA-WS65-010620/974

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may leak information randomly. Affected product versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than 9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00AY Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00BX Versions		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier than 10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		
honor_10_lite					
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in some Huawei products. An unauthenticated, adjacent attacker could exploit this vulnerability to decrypt	N/A	H-HUA-HONO-010620/975

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			data. Successful exploitation may leak information randomly. Affected product versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than 9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00AY Versions earlier than 10.0.0.158(C00E64R1P9);		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Marie-AL00BX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		
cd16-10					
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in some Huawei products. An unauthenticated, adjacent attacker could exploit this	N/A	H-HUA-CD16-010620/976

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to decrypt data. Successful exploitation may leak information randomly. Affected product versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than 9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00AY Versions earlier than		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.0.0.158(C00E64R1P9); Marie-AL00BX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		
cd17-10					
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in some Huawei products. An unauthenticated, adjacent	N/A	H-HUA-CD17-010620/977

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability to decrypt data. Successful exploitation may leak information randomly. Affected product versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than 9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00AY Versions		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier than 10.0.0.158(C00E64R1P9); Marie-AL00BX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		
cd18-10					
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in some Huawei products. An	N/A	H-HUA-CD18-010620/978

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, adjacent attacker could exploit this vulnerability to decrypt data. Successful exploitation may leak information randomly. Affected product versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than 9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than 10.0.0.158(C00E64R1P9);		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Marie-AL00AY Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00BX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		
ws5200-11					
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in	N/A	H-HUA-WS52-010620/979

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			some Huawei products. An unauthenticated, adjacent attacker could exploit this vulnerability to decrypt data. Successful exploitation may leak information randomly. Affected product versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than 10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than 9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.0.0.158(C00E64R1P9); Marie-AL00AY Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00BX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than 10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		
p30					
Improper	29-05-2020	2.1	HUAWEI P30 smartphones	https://w	H-HUA-P30-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication			with versions earlier than 10.1.0.135(C00E135R2P11) have an improper authentication vulnerability. A logic error occurs when handling NFC work, an attacker should establish a NFC connection to the target phone, and then do a series of operations on the target phone. Successful exploit could allow a guest user do certain operation which is beyond the guest user's privilege. **CVE ID : CVE-2020-1798**	ww.huawei.com/en/psirt/security-advisories/huawei-sa-20200527-02-smartphone-en	010620/980
ws6500-10					
Information Exposure	21-05-2020	3.3	There is an information leakage vulnerability in some Huawei products. An unauthenticated, adjacent attacker could exploit this vulnerability to decrypt data. Successful exploitation may leak information randomly. Affected product versions include: Anne-AL00 Versions earlier than 9.1.0.331(C675E9R1P3T8); Berkeley-L09 Versions earlier than 10.0.1.1(C675R1); CD16-10 Versions earlier than 10.0.2.8; CD17-10 Versions earlier than 10.0.2.8; CD17-16 Versions earlier than 10.0.2.8; CD18-10 Versions earlier than 10.0.2.8; CD18-16 Versions earlier than	N/A	H-HUA-WS65-010620/981

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.0.2.8; Columbia-TL00B Versions earlier than 9.0.0.187(C01E181R1P20T8); E6878-370 Versions earlier than 10.0.5.1(H610SP10C00); HUAWEI P30 lite Versions earlier than 10.0.0.185(C605E3R1P3), Versions earlier than 10.0.0.197(C432E8R2P7); HUAWEI nova 4e Versions earlier than 10.0.0.158(C00E64R1P9); Honor 10 Lite 9.0.1.113(C675E11R1P12); LelandP-L22A Versions earlier than 9.1.0.166(C675E5R1P4T8); Marie-AL00AX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00AY Versions earlier than 10.0.0.158(C00E64R1P9); Marie-AL00BX Versions earlier than 10.0.0.158(C00E64R1P9); Marie-L03BX Versions earlier than 10.0.0.188(C605E5R1P1); Marie-L21BX Versions earlier than 10.0.0.188(C432E4R4P1), Versions earlier than 10.0.0.188(C461E5R3P1); Marie-L22BX Versions earlier than 10.0.0.188(C636E3R3P1); Marie-L23BX Versions earlier than		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.0.0.188(C605E5R1P1); TC5200-16 Versions earlier than 10.0.2.8; WS5200-11 Versions earlier than 10.0.2.8; WS5200-12 Versions earlier than 10.0.2.23; WS5200-16 Versions earlier than 10.0.2.8; WS5200-17 Versions earlier than 10.0.2.23; WS5800-10 Versions earlier than 10.0.3.27; WS6500-10 Versions earlier than 10.0.2.8; WS6500-16 Versions earlier than 10.0.2.8 **CVE ID : CVE-2020-9069**		
IBM					
security_access_manager_appliance					
Improper Input Validation	20-05-2020	4	IBM Security Access Manager Appliance 9.0.7.1 could allow an authenticated user to bypass security by allowing id_token claims manipulation without verification. IBM X-Force ID: 181481. **CVE ID : CVE-2020-4461**	https://www.ibm.com/support/pages/node/6211847	H-IBM-SECU-010620/982
Lenovo					
lj6700dn					
Improper Input Validation	28-05-2020	7.8	A denial of service vulnerability was reported in the firmware prior to version 1.01 used in Lenovo Printer LJ4010DN that could be triggered by a remote user sending a	https://iknow.lenovo.com.cn/detail/dc_188830.html	H-LEN-LJ67-010620/983

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted packet to the device, causing an error to be displayed and preventing printer from functioning until the printer is rebooted. **CVE ID : CVE-2020-8329**		
Improper Input Validation	28-05-2020	7.8	A denial of service vulnerability was reported in the firmware prior to version 1.01 used in Lenovo Printer LJ4010DN that could be triggered by a remote user sending a crafted packet to the device, preventing subsequent print jobs until the printer is rebooted. **CVE ID : CVE-2020-8330**	https://iknow.lenovo.com.cn/detail/dc_188830.html	H-LEN-LJ67-010620/984
m8960dnf					
Improper Input Validation	28-05-2020	7.8	A denial of service vulnerability was reported in the firmware prior to version 1.01 used in Lenovo Printer LJ4010DN that could be triggered by a remote user sending a crafted packet to the device, causing an error to be displayed and preventing printer from functioning until the printer is rebooted. **CVE ID : CVE-2020-8329**	https://iknow.lenovo.com.cn/detail/dc_188830.html	H-LEN-M896-010620/985
Improper Input Validation	28-05-2020	7.8	A denial of service vulnerability was reported in the firmware prior to version 1.01 used in Lenovo Printer LJ4010DN that	https://iknow.lenovo.com.cn/detail/dc_188830.	H-LEN-M896-010620/986

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could be triggered by a remote user sending a crafted packet to the device, preventing subsequent print jobs until the printer is rebooted. **CVE ID : CVE-2020-8330**	html	
lj4010dn					
Improper Input Validation	28-05-2020	7.8	A denial of service vulnerability was reported in the firmware prior to version 1.01 used in Lenovo Printer LJ4010DN that could be triggered by a remote user sending a crafted packet to the device, causing an error to be displayed and preventing printer from functioning until the printer is rebooted. **CVE ID : CVE-2020-8329**	https://iknow.lenovo.com.cn/detail/dc_188830.html	H-LEN-LJ40-010620/987
Improper Input Validation	28-05-2020	7.8	A denial of service vulnerability was reported in the firmware prior to version 1.01 used in Lenovo Printer LJ4010DN that could be triggered by a remote user sending a crafted packet to the device, preventing subsequent print jobs until the printer is rebooted. **CVE ID : CVE-2020-8330**	https://iknow.lenovo.com.cn/detail/dc_188830.html	H-LEN-LJ40-010620/988
Netgear					
r6220					
Improper Certificate	28-05-2020	4.3	Certain NETGEAR devices are affected by Missing SSL	N/A	H-NET-R622-010620/989

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Certificate Validation. This affects R7000 1.0.9.6_1.2.19 through 1.0.11.100_10.2.10, and possibly R6120, R7800, R6220, R8000, R6350, R9000, R6400, RAX120, R6400v2, RBR20, R6800, XR300, R6850, XR500, and R7000P. **CVE ID : CVE-2020-13245**		
r6800					
Improper Certificate Validation	28-05-2020	4.3	Certain NETGEAR devices are affected by Missing SSL Certificate Validation. This affects R7000 1.0.9.6_1.2.19 through 1.0.11.100_10.2.10, and possibly R6120, R7800, R6220, R8000, R6350, R9000, R6400, RAX120, R6400v2, RBR20, R6800, XR300, R6850, XR500, and R7000P. **CVE ID : CVE-2020-13245**	N/A	H-NET-R680-010620/990
r6120					
Improper Certificate Validation	28-05-2020	4.3	Certain NETGEAR devices are affected by Missing SSL Certificate Validation. This affects R7000 1.0.9.6_1.2.19 through 1.0.11.100_10.2.10, and possibly R6120, R7800, R6220, R8000, R6350, R9000, R6400, RAX120, R6400v2, RBR20, R6800, XR300, R6850, XR500, and R7000P. **CVE ID : CVE-2020-13245**	N/A	H-NET-R612-010620/991
r6350					
Improper	28-05-2020	4.3	Certain NETGEAR devices	N/A	H-NET-R635-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Certificate Validation			are affected by Missing SSL Certificate Validation. This affects R7000 1.0.9.6_1.2.19 through 1.0.11.100_10.2.10, and possibly R6120, R7800, R6220, R8000, R6350, R9000, R6400, RAX120, R6400v2, RBR20, R6800, XR300, R6850, XR500, and R7000P. **CVE ID : CVE-2020-13245**		010620/992
r6850					
Improper Certificate Validation	28-05-2020	4.3	Certain NETGEAR devices are affected by Missing SSL Certificate Validation. This affects R7000 1.0.9.6_1.2.19 through 1.0.11.100_10.2.10, and possibly R6120, R7800, R6220, R8000, R6350, R9000, R6400, RAX120, R6400v2, RBR20, R6800, XR300, R6850, XR500, and R7000P. **CVE ID : CVE-2020-13245**	N/A	H-NET-R685-010620/993
xr300					
Improper Certificate Validation	28-05-2020	4.3	Certain NETGEAR devices are affected by Missing SSL Certificate Validation. This affects R7000 1.0.9.6_1.2.19 through 1.0.11.100_10.2.10, and possibly R6120, R7800, R6220, R8000, R6350, R9000, R6400, RAX120, R6400v2, RBR20, R6800, XR300, R6850, XR500, and R7000P. **CVE ID : CVE-2020-13245**	N/A	H-NET-XR30-010620/994
rbs50y					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	18-05-2020	8.3	An issue was discovered on NETGEAR Orbi Tri-Band Business WiFi Add-on Satellite (SRS60) AC3000 V2.5.1.106, Outdoor Satellite (RBS50Y) V2.5.1.106, and Pro Tri-Band Business WiFi Router (SRR60) AC3000 V2.5.1.106. The root account has the same password as the Web-admin component. Thus, by exploiting CVE-2020-11551, it is possible to achieve remote code execution with root privileges on the embedded Linux system. **CVE ID : CVE-2020-11549**	N/A	H-NET-RBS5-010620/995
Information Exposure	18-05-2020	3.3	An issue was discovered on NETGEAR Orbi Tri-Band Business WiFi Add-on Satellite (SRS60) AC3000 V2.5.1.106, Outdoor Satellite (RBS50Y) V2.5.1.106, and Pro Tri-Band Business WiFi Router (SRR60) AC3000 V2.5.1.106. The administrative SOAP interface allows an unauthenticated remote leak of sensitive/arbitrary Wi-Fi information, such as SSIDs and Pre-Shared-Keys (PSK). **CVE ID : CVE-2020-11550**	N/A	H-NET-RBS5-010620/996
Improper Authentication	18-05-2020	5.8	An issue was discovered on NETGEAR Orbi Tri-Band Business WiFi Add-on	N/A	H-NET-RBS5-010620/997

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Satellite (SRS60) AC3000 V2.5.1.106, Outdoor Satellite (RBS50Y) V2.5.1.106, and Pro Tri-Band Business WiFi Router (SRR60) AC3000 V2.5.1.106. The administrative SOAP interface allows an unauthenticated remote write of arbitrary Wi-Fi configuration data such as authentication details (e.g., the Web-admin password), network settings, DNS settings, system administration interface configuration, etc. **CVE ID : CVE-2020-11551**		
srr60					
Use of Hard-coded Credentials	18-05-2020	8.3	An issue was discovered on NETGEAR Orbi Tri-Band Business WiFi Add-on Satellite (SRS60) AC3000 V2.5.1.106, Outdoor Satellite (RBS50Y) V2.5.1.106, and Pro Tri-Band Business WiFi Router (SRR60) AC3000 V2.5.1.106. The root account has the same password as the Web-admin component. Thus, by exploiting CVE-2020-11551, it is possible to achieve remote code execution with root privileges on the embedded Linux system. **CVE ID : CVE-2020-11549**	N/A	H-NET-SRR6-010620/998

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	18-05-2020	3.3	An issue was discovered on NETGEAR Orbi Tri-Band Business WiFi Add-on Satellite (SRS60) AC3000 V2.5.1.106, Outdoor Satellite (RBS50Y) V2.5.1.106, and Pro Tri-Band Business WiFi Router (SRR60) AC3000 V2.5.1.106. The administrative SOAP interface allows an unauthenticated remote leak of sensitive/arbitrary Wi-Fi information, such as SSIDs and Pre-Shared-Keys (PSK). **CVE ID : CVE-2020-11550**	N/A	H-NET-SRR6-010620/999
Improper Authentication	18-05-2020	5.8	An issue was discovered on NETGEAR Orbi Tri-Band Business WiFi Add-on Satellite (SRS60) AC3000 V2.5.1.106, Outdoor Satellite (RBS50Y) V2.5.1.106, and Pro Tri-Band Business WiFi Router (SRR60) AC3000 V2.5.1.106. The administrative SOAP interface allows an unauthenticated remote write of arbitrary Wi-Fi configuration data such as authentication details (e.g., the Web-admin password), network settings, DNS settings, system administration interface configuration, etc. **CVE ID : CVE-2020-11551**	N/A	H-NET-SRR6-010620/1000

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
srs60					
Use of Hard-coded Credentials	18-05-2020	8.3	An issue was discovered on NETGEAR Orbi Tri-Band Business WiFi Add-on Satellite (SRS60) AC3000 V2.5.1.106, Outdoor Satellite (RBS50Y) V2.5.1.106, and Pro Tri-Band Business WiFi Router (SRR60) AC3000 V2.5.1.106. The root account has the same password as the Web-admin component. Thus, by exploiting CVE-2020-11551, it is possible to achieve remote code execution with root privileges on the embedded Linux system. **CVE ID : CVE-2020-11549**	N/A	H-NET-SRS6-010620/1001
Information Exposure	18-05-2020	3.3	An issue was discovered on NETGEAR Orbi Tri-Band Business WiFi Add-on Satellite (SRS60) AC3000 V2.5.1.106, Outdoor Satellite (RBS50Y) V2.5.1.106, and Pro Tri-Band Business WiFi Router (SRR60) AC3000 V2.5.1.106. The administrative SOAP interface allows an unauthenticated remote leak of sensitive/arbitrary Wi-Fi information, such as SSIDs and Pre-Shared-Keys (PSK). **CVE ID : CVE-2020-11550**	N/A	H-NET-SRS6-010620/1002
Improper	18-05-2020	5.8	An issue was discovered on NETGEAR Orbi Tri-Band	N/A	H-NET-SRS6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication			Business WiFi Add-on Satellite (SRS60) AC3000 V2.5.1.106, Outdoor Satellite (RBS50Y) V2.5.1.106, and Pro Tri-Band Business WiFi Router (SRR60) AC3000 V2.5.1.106. The administrative SOAP interface allows an unauthenticated remote write of arbitrary Wi-Fi configuration data such as authentication details (e.g., the Web-admin password), network settings, DNS settings, system administration interface configuration, etc. **CVE ID : CVE-2020-11551**		010620/1003
r8000					
Improper Certificate Validation	28-05-2020	4.3	Certain NETGEAR devices are affected by Missing SSL Certificate Validation. This affects R7000 1.0.9.6_1.2.19 through 1.0.11.100_10.2.10, and possibly R6120, R7800, R6220, R8000, R6350, R9000, R6400, RAX120, R6400v2, RBR20, R6800, XR300, R6850, XR500, and R7000P. **CVE ID : CVE-2020-13245**	N/A	H-NET-R800-010620/1004
r6400					
Improper Certificate Validation	28-05-2020	4.3	Certain NETGEAR devices are affected by Missing SSL Certificate Validation. This affects R7000 1.0.9.6_1.2.19 through 1.0.11.100_10.2.10,	N/A	H-NET-R640-010620/1005

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and possibly R6120, R7800, R6220, R8000, R6350, R9000, R6400, RAX120, R6400v2, RBR20, R6800, XR300, R6850, XR500, and R7000P. **CVE ID : CVE-2020-13245**		
r7000p					
Improper Certificate Validation	28-05-2020	4.3	Certain NETGEAR devices are affected by Missing SSL Certificate Validation. This affects R7000 1.0.9.6_1.2.19 through 1.0.11.100_10.2.10, and possibly R6120, R7800, R6220, R8000, R6350, R9000, R6400, RAX120, R6400v2, RBR20, R6800, XR300, R6850, XR500, and R7000P. **CVE ID : CVE-2020-13245**	N/A	H-NET-R700-010620/1006
r7800					
Improper Certificate Validation	28-05-2020	4.3	Certain NETGEAR devices are affected by Missing SSL Certificate Validation. This affects R7000 1.0.9.6_1.2.19 through 1.0.11.100_10.2.10, and possibly R6120, R7800, R6220, R8000, R6350, R9000, R6400, RAX120, R6400v2, RBR20, R6800, XR300, R6850, XR500, and R7000P. **CVE ID : CVE-2020-13245**	N/A	H-NET-R780-010620/1007
r9000					
Improper Certificate Validation	28-05-2020	4.3	Certain NETGEAR devices are affected by Missing SSL Certificate Validation. This affects R7000 1.0.9.6_1.2.19	N/A	H-NET-R900-010620/1008

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			through 1.0.11.100_10.2.10, and possibly R6120, R7800, R6220, R8000, R6350, R9000, R6400, RAX120, R6400v2, RBR20, R6800, XR300, R6850, XR500, and R7000P. **CVE ID : CVE-2020-13245**		
rax120					
Improper Certificate Validation	28-05-2020	4.3	Certain NETGEAR devices are affected by Missing SSL Certificate Validation. This affects R7000 1.0.9.6_1.2.19 through 1.0.11.100_10.2.10, and possibly R6120, R7800, R6220, R8000, R6350, R9000, R6400, RAX120, R6400v2, RBR20, R6800, XR300, R6850, XR500, and R7000P. **CVE ID : CVE-2020-13245**	N/A	H-NET-RAX1-010620/1009
xr500					
Improper Certificate Validation	28-05-2020	4.3	Certain NETGEAR devices are affected by Missing SSL Certificate Validation. This affects R7000 1.0.9.6_1.2.19 through 1.0.11.100_10.2.10, and possibly R6120, R7800, R6220, R8000, R6350, R9000, R6400, RAX120, R6400v2, RBR20, R6800, XR300, R6850, XR500, and R7000P. **CVE ID : CVE-2020-13245**	N/A	H-NET-XR50-010620/1010
rbr20					
Improper Certificate Validation	28-05-2020	4.3	Certain NETGEAR devices are affected by Missing SSL Certificate Validation. This	N/A	H-NET-RBR2-010620/1011

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affects R7000 1.0.9.6_1.2.19 through 1.0.11.100_10.2.10, and possibly R6120, R7800, R6220, R8000, R6350, R9000, R6400, RAX120, R6400v2, RBR20, R6800, XR300, R6850, XR500, and R7000P. **CVE ID : CVE-2020-13245**		
nintendo					
nintendo_64					
Out-of-bounds Write	16-05-2020	7.5	Morita Shogi 64 through 2020-05-02 for Nintendo 64 devices allows remote attackers to execute arbitrary code via crafted packet data to the built-in modem because 0x800b3e94 (aka the IF subcommand to top-level command 7) has a stack-based buffer overflow. **CVE ID : CVE-2020-13109**	N/A	H-NIN-NINT-010620/1012
Panasonic					
p99					
N/A	19-05-2020	7.5	Panasonic P99 devices through 2020-04-10 have Incorrect Access Control. NOTE: the vendor states that all affected products are at "End-of-software-support." **CVE ID : CVE-2020-11715**	https://mobile.panasonic.com/in/advisory	H-PAN-P99-010620/1013
p110					
Incorrect Default Permissions	20-05-2020	7.5	Panasonic P110, Eluga Z1 Pro, Eluga X1, and Eluga X1 Pro devices through 2020-04-10 have Insecure	https://mobile.panasonic.com/in/advis	H-PAN-P110-010620/1014

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Permissions. NOTE: the vendor states that all affected products are at "End-of-software-support." **CVE ID : CVE-2020-11716**	ory	
eluga_z1_pro					
Incorrect Default Permissions	20-05-2020	7.5	Panasonic P110, Eluga Z1 Pro, Eluga X1, and Eluga X1 Pro devices through 2020-04-10 have Insecure Permissions. NOTE: the vendor states that all affected products are at "End-of-software-support." **CVE ID : CVE-2020-11716**	https://mobile.panasonic.com/in/advisory	H-PAN-ELUG-010620/1015
eluga_x1					
Incorrect Default Permissions	20-05-2020	7.5	Panasonic P110, Eluga Z1 Pro, Eluga X1, and Eluga X1 Pro devices through 2020-04-10 have Insecure Permissions. NOTE: the vendor states that all affected products are at "End-of-software-support." **CVE ID : CVE-2020-11716**	https://mobile.panasonic.com/in/advisory	H-PAN-ELUG-010620/1016
eluga_x1_pro					
Incorrect Default Permissions	20-05-2020	7.5	Panasonic P110, Eluga Z1 Pro, Eluga X1, and Eluga X1 Pro devices through 2020-04-10 have Insecure Permissions. NOTE: the vendor states that all affected products are at "End-of-software-support." **CVE ID : CVE-2020-11716**	https://mobile.panasonic.com/in/advisory	H-PAN-ELUG-010620/1017
eluga_ray_530					
Incorrect	20-05-2020	7.5	Panasonic P110, Eluga Z1	https://m	H-PAN-ELUG-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Default Permissions			Pro, Eluga X1, and Eluga X1 Pro devices through 2020-04-10 have Insecure Permissions. NOTE: the vendor states that all affected products are at "End-of-software-support." **CVE ID : CVE-2020-11716**	obile.panasonic.com/in/advisory	010620/1018
eluga_ray_600					
Incorrect Default Permissions	20-05-2020	7.5	Panasonic P110, Eluga Z1 Pro, Eluga X1, and Eluga X1 Pro devices through 2020-04-10 have Insecure Permissions. NOTE: the vendor states that all affected products are at "End-of-software-support." **CVE ID : CVE-2020-11716**	https://mobile.panasonic.com/in/advisory	H-PAN-ELUG-010620/1019
Tendacn					
ac6					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/SetNetControlList list parameter for a POST request, a value is directly used in a strcpy to a local	N/A	H-TEN-AC6-010620/1020

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13394**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/openSchedWifi schedStartTime and schedEndTime parameters for a POST request, a value is directly used in a strcpy to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13389**	N/A	H-TEN-AC6-010620/1021
Buffer Copy without Checking Size of Input	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0	N/A	H-TEN-AC6-010620/1022

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/addressNat entrys and mitInterface parameters for a POST request, a value is directly used in a sprintf to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13390**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/SetSpeedWan speed_dir parameter for a	N/A	H-TEN-AC6-010620/1023

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			POST request, a value is directly used in a sprintf to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13391**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/setcfm funcpara1 parameter for a POST request, a value is directly used in a sprintf to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13392**	N/A	H-TEN-AC6-010620/1024
Buffer Copy without Checking Size	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01,	N/A	H-TEN-AC6-010620/1025

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/saveParentControlInfo deviceId and time parameters for a POST request, a value is directly used in a strcpy to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13393**		
ac9					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server --	N/A	H-TEN-AC9-010620/1026

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			httpd. While processing the /goform/SetNetControlList list parameter for a POST request, a value is directly used in a strcpy to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13394**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/openSchedWifi schedStartTime and schedEndTime parameters for a POST request, a value is directly used in a strcpy to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks.	N/A	H-TEN-AC9-010620/1027

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-13389		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/addressNat entrys and mitInterface parameters for a POST request, a value is directly used in a sprintf to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13390**	N/A	H-TEN-AC9-010620/1028
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN	N/A	H-TEN-AC9-010620/1029

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/SetSpeedWan speed_dir parameter for a POST request, a value is directly used in a sprintf to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13391**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/setcfm funcpara1 parameter for a POST request, a value is directly used in a sprintf to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution	N/A	H-TEN-AC9-010620/1030

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks. **CVE ID : CVE-2020-13392**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/saveParentControlInfo deviceId and time parameters for a POST request, a value is directly used in a strcpy to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13393**	N/A	H-TEN-AC9-010620/1031
ac15					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01,	N/A	H-TEN-AC15-010620/1032

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/SetNetControlList list parameter for a POST request, a value is directly used in a strcpy to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13394**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/openSchedWifi schedStartTime and schedEndTime parameters for a POST request, a value is directly used in a strcpy to a local variable placed on the stack, which overwrites the return address of a	N/A	H-TEN-AC15-010620/1033

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13389**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/addressNat entrys and mitInterface parameters for a POST request, a value is directly used in a sprintf to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13390**	N/A	H-TEN-AC15-010620/1034
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15	N/A	H-TEN-AC15-010620/1035

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/SetSpeedWan speed_dir parameter for a POST request, a value is directly used in a sprintf to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13391**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/setcfm funcpara1 parameter for a POST request, a value is directly used in a sprintf to a local variable placed on the stack, which overwrites the return	N/A	H-TEN-AC15-010620/1036

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13392**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/saveParentControlInfo deviceId and time parameters for a POST request, a value is directly used in a strcpy to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13393**	N/A	H-TEN-AC15-010620/1037
ac18					
Buffer Copy without Checking Size of Input ('Classic Buffer	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN,	N/A	H-TEN-AC18-010620/1038

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/SetNetControlList list parameter for a POST request, a value is directly used in a strcpy to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13394**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/openSchedWifi schedStartTime and schedEndTime parameters for a POST request, a value	N/A	H-TEN-AC18-010620/1039

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is directly used in a strcpy to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13389**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/addressNat entrys and mitInterface parameters for a POST request, a value is directly used in a sprintf to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13390**	N/A	H-TEN-AC18-010620/1040
Buffer Copy without Checking Size	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01,	N/A	H-TEN-AC18-010620/1041

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/SetSpeedWan speed_dir parameter for a POST request, a value is directly used in a sprintf to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13391**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/setcfm funcpara1 parameter for a POST	N/A	H-TEN-AC18-010620/1042

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request, a value is directly used in a sprintf to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13392**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-05-2020	7.5	An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318)_CN, AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, and AC18 V15.03.05.19(6318_)_CN devices. There is a buffer overflow vulnerability in the router's web server -- httpd. While processing the /goform/saveParentControlInfo deviceId and time parameters for a POST request, a value is directly used in a strcpy to a local variable placed on the stack, which overwrites the return address of a function. An attacker can construct a payload to carry out arbitrary code execution attacks. **CVE ID : CVE-2020-13393**	N/A	H-TEN-AC18-010620/1043
thetrackr					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
trackr					
Missing Authorization	23-05-2020	6.8	TrackR devices through 2020-05-06 allow attackers to trigger the Beep (aka alarm) feature, which will eventually cause a denial of service when battery capacity is exhausted. **CVE ID : CVE-2020-13425**	N/A	H-THE-TRAC-010620/1044
ui					
ag-hp-2g16					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**	N/A	H-UI-AG-H-010620/1045

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**	N/A	H-UI-AG-H-010620/1046
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS	N/A	H-UI-AG-H-010620/1047

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**		
ag-hp-2g20					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**	N/A	H-UI-AG-H-010620/1048
Improper Neutralization of Input During Web Page Generation ('Cross-site	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards,	N/A	H-UI-AG-H-010620/1049

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**	N/A	H-UI-AG-H-010620/1050
ag-hp-5g23					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**	N/A	H-UI-AG-H-010620/1051
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user'	N/A	H-UI-AG-H-010620/1052

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**	N/A	H-UI-AG-H-010620/1053
ag-hp-5g27					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards,	N/A	H-UI-AG-H-010620/1054

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download	N/A	H-UI-AG-H-010620/1055

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			page. **CVE ID : CVE-2020-8170**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**	N/A	H-UI-AG-H-010620/1056
airgrid_m					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit	N/A	H-UI-AIRG-010620/1057

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**	N/A	H-UI-AIRG-010620/1058
Improper Neutralization of Special Elements used	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that	N/A	H-UI-AIRG-010620/1059

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
in an OS Command ('OS Command Injection')			fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**		
airgrid_m2					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration,	N/A	H-UI-AIRG-010620/1060

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**	N/A	H-UI-AIRG-010620/1061
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing	N/A	H-UI-AIRG-010620/1062

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**		
airgrid_m5					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download	N/A	H-UI-AIRG-010620/1063

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			page. **CVE ID : CVE-2020-8168**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**	N/A	H-UI-AIRG-010620/1064
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands,	N/A	H-UI-AIRG-010620/1065

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**		
ar					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**	N/A	H-UI-AR-010620/1066
Improper Neutralization of Input During Web Page	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that	N/A	H-UI-AR-010620/1067

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page.	N/A	H-UI-AR-010620/1068

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8171		
ar-hp					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**	N/A	H-UI-AR-H-010620/1069
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable	N/A	H-UI-AR-H-010620/1070

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**	N/A	H-UI-AR-H-010620/1071
bm2-ti					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that	N/A	H-UI-BM2--010620/1072

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to	N/A	H-UI-BM2--010620/1073

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**	N/A	H-UI-BM2--010620/1074
bm2hp					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site	N/A	H-UI-BM2H-010620/1075

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**	N/A	H-UI-BM2H-010620/1076
Improper	26-05-2020	7.5	We have recently released	N/A	H-UI-BM2H-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in an OS Command ('OS Command Injection')			new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**		010620/1077
bm5-ti					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as	N/A	H-UI-BM5--010620/1078

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**	N/A	H-UI-BM5--010620/1079
Improper Neutralization of Special Elements used in an OS Command ('OS Command	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards,	N/A	H-UI-BM5--010620/1080

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**		
bm5hp					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to	N/A	H-UI-BM5H-010620/1081

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**	N/A	H-UI-BM5H-010620/1082
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to	N/A	H-UI-BM5H-010620/1083

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**		
is-m5					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**	N/A	H-UI-IS-M-010620/1084

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**	N/A	H-UI-IS-M-010620/1085
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS	N/A	H-UI-IS-M-010620/1086

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**		
lbem5-23					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**	N/A	H-UI-LBEM-010620/1087
Improper Neutralization of Input During Web Page Generation ('Cross-site	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards,	N/A	H-UI-LBEM-010620/1088

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**	N/A	H-UI-LBEM-010620/1089
litestation_m5					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**	N/A	H-UI-LITE-010620/1090
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user'	N/A	H-UI-LITE-010620/1091

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**	N/A	H-UI-LITE-010620/1092
locom2					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards,	N/A	H-UI-LOCO-010620/1093

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download	N/A	H-UI-LOCO-010620/1094

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			page. **CVE ID : CVE-2020-8170**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**	N/A	H-UI-LOCO-010620/1095
locom5					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit	N/A	H-UI-LOCO-010620/1096

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**	N/A	H-UI-LOCO-010620/1097
Improper Neutralization of Special Elements used	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that	N/A	H-UI-LOCO-010620/1098

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
in an OS Command ('OS Command Injection')			fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**		
locom9					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration,	N/A	H-UI-LOCO-010620/1099

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**	N/A	H-UI-LOCO-010620/1100
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing	N/A	H-UI-LOCO-010620/1101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**		
m2					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download	N/A	H-UI-M2-010620/1102

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			page. **CVE ID : CVE-2020-8168**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**	N/A	H-UI-M2-010620/1103
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands,	N/A	H-UI-M2-010620/1104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**		
m3					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**	N/A	H-UI-M3-010620/1105
Improper Neutralization of Input During Web Page	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that	N/A	H-UI-M3-010620/1106

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page.	N/A	H-UI-M3-010620/1107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8171		
m365					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**	N/A	H-UI-M365-010620/1108
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable	N/A	H-UI-M365-010620/1109

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**	N/A	H-UI-M365-010620/1110
m5					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that	N/A	H-UI-M5-010620/1111

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to	N/A	H-UI-M5-010620/1112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**	N/A	H-UI-M5-010620/1113
m900					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site	N/A	H-UI-M900-010620/1114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**	N/A	H-UI-M900-010620/1115
Improper	26-05-2020	7.5	We have recently released	N/A	H-UI-M900-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in an OS Command ('OS Command Injection')			new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**		010620/1116
nb-2g18					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as	N/A	H-UI-NB-2-010620/1117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**	N/A	H-UI-NB-2-010620/1118
Improper Neutralization of Special Elements used in an OS Command ('OS Command	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards,	N/A	H-UI-NB-2-010620/1119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**		
nb-5g22					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to	N/A	H-UI-NB-5-010620/1120

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**	N/A	H-UI-NB-5-010620/1121
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to	N/A	H-UI-NB-5-010620/1122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**		
nb-5g25					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**	N/A	H-UI-NB-5-010620/1123

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**	N/A	H-UI-NB-5-010620/1124
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS	N/A	H-UI-NB-5-010620/1125

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**		
nbe-m2-13					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**	N/A	H-UI-NBE--010620/1126
Improper Neutralization of Input During Web Page Generation ('Cross-site	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards,	N/A	H-UI-NBE--010620/1127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**	N/A	H-UI-NBE--010620/1128
nbe-m5-16					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**	N/A	H-UI-NBE--010620/1129
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user'	N/A	H-UI-NBE--010620/1130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**	N/A	H-UI-NBE--010620/1131
nbe-m5-19					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards,	N/A	H-UI-NBE--010620/1132

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download	N/A	H-UI-NBE--010620/1133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			page. **CVE ID : CVE-2020-8170**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**	N/A	H-UI-NBE--010620/1134
nbm3					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit	N/A	H-UI-NBM3-010620/1135

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**	N/A	H-UI-NBM3-010620/1136
Improper Neutralization of Special Elements used	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that	N/A	H-UI-NBM3-010620/1137

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
in an OS Command ('OS Command Injection')			fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**		
nbm365					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration,	N/A	H-UI-NBM3-010620/1138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**	N/A	H-UI-NBM3-010620/1139
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing	N/A	H-UI-NBM3-010620/1140

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**		
nbm9					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download	N/A	H-UI-NBM9-010620/1141

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			page. **CVE ID : CVE-2020-8168**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**	N/A	H-UI-NBM9-010620/1142
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands,	N/A	H-UI-NBM9-010620/1143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**		
nsm2					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**	N/A	H-UI-NSM2-010620/1144
Improper Neutralization of Input During Web Page	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that	N/A	H-UI-NSM2-010620/1145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page.	N/A	H-UI-NSM2-010620/1146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8171		
nsm3					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**	N/A	H-UI-NSM3-010620/1147
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable	N/A	H-UI-NSM3-010620/1148

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**	N/A	H-UI-NSM3-010620/1149
nsm365					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that	N/A	H-UI-NSM3-010620/1150

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to	N/A	H-UI-NSM3-010620/1151

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**	N/A	H-UI-NSM3-010620/1152
nsm5					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site	N/A	H-UI-NSM5-010620/1153

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**	N/A	H-UI-NSM5-010620/1154
Improper	26-05-2020	7.5	We have recently released	N/A	H-UI-NSM5-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in an OS Command ('OS Command Injection')			new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**		010620/1155
pbe-m2-400					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as	N/A	H-UI-PBE--010620/1156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**	N/A	H-UI-PBE--010620/1157
Improper Neutralization of Special Elements used in an OS Command ('OS Command	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards,	N/A	H-UI-PBE--010620/1158

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**		
pbe-m5-300					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to	N/A	H-UI-PBE--010620/1159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**	N/A	H-UI-PBE--010620/1160
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to	N/A	H-UI-PBE--010620/1161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**		
pbe-m5-300-iso					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**	N/A	H-UI-PBE--010620/1162

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**	N/A	H-UI-PBE--010620/1163
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS	N/A	H-UI-PBE--010620/1164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**		
pbe-m5-400					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**	N/A	H-UI-PBE--010620/1165
Improper Neutralization of Input During Web Page Generation ('Cross-site	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards,	N/A	H-UI-PBE--010620/1166

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**	N/A	H-UI-PBE--010620/1167
pbe-m5-400-iso					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**	N/A	H-UI-PBE--010620/1168
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user'	N/A	H-UI-PBE--010620/1169

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**	N/A	H-UI-PBE--010620/1170
pbe-m5-620					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards,	N/A	H-UI-PBE--010620/1171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download	N/A	H-UI-PBE--010620/1172

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			page. **CVE ID : CVE-2020-8170**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**	N/A	H-UI-PBE--010620/1173
pbm10					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit	N/A	H-UI-PBM1-010620/1174

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**	N/A	H-UI-PBM1-010620/1175
Improper Neutralization of Special Elements used	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that	N/A	H-UI-PBM1-010620/1176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
in an OS Command ('OS Command Injection')			fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**		
pbm365					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration,	N/A	H-UI-PBM3-010620/1177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**	N/A	H-UI-PBM3-010620/1178
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing	N/A	H-UI-PBM3-010620/1179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**		
pbm5					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download	N/A	H-UI-PBM5-010620/1180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			page. **CVE ID : CVE-2020-8168**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**	N/A	H-UI-PBM5-010620/1181
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands,	N/A	H-UI-PBM5-010620/1182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**		
picom2hp					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**	N/A	H-UI-PICO-010620/1183
Improper Neutralization of Input During Web Page	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that	N/A	H-UI-PICO-010620/1184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page.	N/A	H-UI-PICO-010620/1185

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8171		
power_ap_n					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**	N/A	H-UI-POWE-010620/1186
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable	N/A	H-UI-POWE-010620/1187

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**	N/A	H-UI-POWE-010620/1188
rm2-ti					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that	N/A	H-UI-RM2--010620/1189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to	N/A	H-UI-RM2--010620/1190

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-05-2020	7.5	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**	N/A	H-UI-RM2--010620/1191
rm5-ti					
Cross-Site Request Forgery (CSRF)	26-05-2020	6.8	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Attackers can abuse multiple end-points not protected against cross-site	N/A	H-UI-RM5--010620/1192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request forgery (CSRF), as a result authenticated users can be persuaded to visit malicious web pages, which allows attackers to perform arbitrary actions, such as downgrade the device's firmware to older versions, modify configuration, upload arbitrary firmware, exfiltrate files and tokens.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8168**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-05-2020	4.3	We have recently released new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:Multiple end-points with parameters vulnerable to reflected cross site scripting (XSS), allowing attackers to abuse the user' session information and/or account takeover of the admin user.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8170**	N/A	H-UI-RM5--010620/1193
Improper	26-05-2020	7.5	We have recently released	N/A	H-UI-RM5--

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in an OS Command ('OS Command Injection')			new version of AirMax AirOS firmware v6.3.0 for TI, XW and XM boards that fixes vulnerabilities found on AirMax AirOS v6.2.0 and prior TI, XW and XM boards, according to the description below:There are certain end-points containing functionalities that are vulnerable to command injection. It is possible to craft an input string that passes the filter check but still contains commands, resulting in remote code execution.Mitigation:Update to the latest AirMax AirOS firmware version available at the AirMax download page. **CVE ID : CVE-2020-8171**		010620/1194