National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures(CVE) Report

01 - 15 Jul 2020 Vol. 07 No. 13

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
ABB					
robotware					
Improper Authentication	7/15/2020	7.5	IRC5 exposes an ftp server (port 21). Upon attempting to gain access you are challenged with a request of username and password, however you can input whatever you like. As long as the field isn't empty it will be accepted. **CVE ID : CVE-2020-10288**	https://github.com/aliasrobotics/RVD/issues/3327	A-ABB-ROBO-100820/1
Advantech					
iview					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	7/15/2020	7.5	Advantech iView, versions 5.6 and prior, contains multiple SQL injection vulnerabilities that are vulnerable to the use of an attacker-controlled string in the construction of SQL queries. An attacker could extract user credentials, read or modify information, and remotely execute code. **CVE ID : CVE-2020-14497**	N/A	A-ADV-IVIE-100820/2
Insufficiently Protected Credentials	7/15/2020	5	Advantech iView, versions 5.6 and prior, has an improper access control vulnerability. Successful exploitation of this	N/A	A-ADV-IVIE-100820/3

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability may allow an attacker to obtain all user accounts credentials. **CVE ID : CVE-2020-14499**		
Missing Authentication for Critical Function	7/15/2020	5	Advantech iView, versions 5.6 and prior, has an improper authentication for critical function (CWE-306) issue. Successful exploitation of this vulnerability may allow an attacker to obtain the information of the user table, including the administrator credentials in plain text. An attacker may also delete the administrator account. **CVE ID : CVE-2020-14501**	N/A	A-ADV-IVIE-100820/4
Improper Input Validation	7/15/2020	7.5	Advantech iView, versions 5.6 and prior, has an improper input validation vulnerability. Successful exploitation of this vulnerability could allow an attacker to remotely execute arbitrary code. **CVE ID : CVE-2020-14503**	N/A	A-ADV-IVIE-100820/5
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	7/15/2020	7.5	Advantech iView, versions 5.6 and prior, has an improper neutralization of special elements used in a command (“command injection”) vulnerability. Successful exploitation of this vulnerability may allow an attacker to send a HTTP GET or POST request that creates a command	N/A	A-ADV-IVIE-100820/6

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			string without any validation. The attacker may then remotely execute code. **CVE ID : CVE-2020-14505**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	7/15/2020	7.5	Advantech iView, versions 5.6 and prior, is vulnerable to multiple path traversal vulnerabilities that could allow an attacker to create/download arbitrary files, limit system availability, and remotely execute code. **CVE ID : CVE-2020-14507**	N/A	A-ADV-IVIE-100820/7
ajv.js					
ajv					
Improper Input Validation	7/15/2020	6.8	An issue was discovered in ajv.validate() in Ajv (aka Another JSON Schema Validator) 6.12.2. A carefully crafted JSON schema could be provided that allows execution of other code by prototype pollution. (While untrusted schemas are recommended against, the worst case of an untrusted schema should be a denial of service, not execution of code.) **CVE ID : CVE-2020-15366**	N/A	A-AJV-AJV-100820/8
Amazon					
tough					
Improper Verification of Cryptographic	7/9/2020	5	The tough library (Rust/crates.io) prior to version 0.7.1 does not	https://github.com/awslabs/tough	A-AMA-TOUG-100820/9

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Signature			properly verify the threshold of cryptographic signatures. It allows an attacker to duplicate a valid signature in order to circumvent TUF requiring a minimum threshold of unique signatures before the metadata is considered valid. A fix is available in version 0.7.1. CVE-2020-6174 is assigned to the same vulnerability in the TUF reference implementation. **CVE ID : CVE-2020-15093**	/security/advisories/GHSA-5q2r-92f9-4m49	
Apache					
tomcat					
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	5	An h2c direct connection to Apache Tomcat 10.0.0-M1 to 10.0.0-M6, 9.0.0.M5 to 9.0.36 and 8.5.1 to 8.5.56 did not release the HTTP/1.1 processor after the upgrade to HTTP/2. If a sufficient number of such requests were made, an OutOfMemoryException could occur leading to a denial of service. **CVE ID : CVE-2020-13934**	https://security.netapp.com/advisory/ntap-20200724-0003/	A-APA-TOMC-100820/10
Loop with Unreachable Exit Condition ('Infinite Loop')	7/14/2020	5	The payload length in a WebSocket frame was not correctly validated in Apache Tomcat 10.0.0-M1 to 10.0.0-M6, 9.0.0.M1 to 9.0.36, 8.5.0 to 8.5.56 and 7.0.27 to 7.0.104. Invalid payload lengths could	https://security.netapp.com/advisory/ntap-20200724-0003/	A-APA-TOMC-100820/11

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			trigger an infinite loop. Multiple requests with invalid payload lengths could lead to a denial of service. **CVE ID : CVE-2020-13935**		
guacamole					
Information Exposure	7/2/2020	1.2	Apache Guacamole 1.1.0 and older do not properly validate datareceived from RDP servers via static virtual channels. If a userconnects to a malicious or compromised RDP server, specially-craftedPDUs could result in disclosure of information within the memory ofthe guacd process handling the connection. **CVE ID : CVE-2020-9497**	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44525	A-APA-GUAC-100820/12
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/2/2020	6.2	Apache Guacamole 1.1.0 and older may mishandle pointers involved inprocessing data received via RDP static virtual channels. If a userconnects to a malicious or compromised RDP server, a series ofspecially-crafted PDUs could result in memory corruption, possiblyallowing arbitrary code to be executed with the privileges of therunning guacd process. **CVE ID : CVE-2020-9498**	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44525	A-APA-GUAC-100820/13
dubbo					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Deserialization of Untrusted Data	7/14/2020	7.5	This vulnerability can affect all Dubbo users stay on version 2.7.6 or lower. An attacker can send RPC requests with unrecognized service name or method name along with some malicious parameter payloads. When the malicious parameter is deserialized, it will execute some malicious code. More details can be found below. **CVE ID : CVE-2020-1948**	N/A	A-APA-DUBB-100820/14
ofbiz					
Improper Input Validation	7/15/2020	5	IDOR vulnerability in the order processing feature from ecommerce component of Apache OFBiz before 17.12.04 **CVE ID : CVE-2020-13923**	N/A	A-APA-OFBI-100820/15
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/15/2020	4.3	XML-RPC request are vulnerable to unsafe deserialization and Cross-Site Scripting issues in Apache OFBiz 17.12.03 **CVE ID : CVE-2020-9496**	N/A	A-APA-OFBI-100820/16
kylin					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	7/14/2020	10	Similar to CVE-2020-1956, Kylin has one more restful API which concatenates the API inputs into OS commands and then executes them on the server; while the reported API misses necessary input validation, which causes the hackers to have the	N/A	A-APA-KYLI-100820/17

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			possibility to execute OS command remotely. Users of all previous versions after 2.3 should upgrade to 3.1.0. **CVE ID : CVE-2020-13925**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	7/14/2020	7.5	Kylin concatenates and executes a Hive SQL in Hive CLI or beeline when building a new segment; some part of the HQL is from system configurations, while the configuration can be overwritten by certain rest api, which makes SQL injection attack is possible. Users of all previous versions after 2.0 should upgrade to 3.1.0. **CVE ID : CVE-2020-13926**	N/A	A-APA-KYLI-100820/18
camel					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	7/8/2020	5	Server-Side Template Injection and arbitrary file disclosure on Camel templating components **CVE ID : CVE-2020-11994**	N/A	A-APA-CAME-100820/19
articatech					
artica_proxy					
Improper Neutralization of Input During Web Page Generation ('Cross-site	7/15/2020	4.3	An issue was discovered in Artica Proxy before 4.30.000000. Stored XSS exists via the Server Domain Name, Your Email Address, Group Name, MYSQL Server, Database,	N/A	A-ART-ARTI-100820/20

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			MYSQL Username, Group Name, and Task Description fields. **CVE ID : CVE-2020-15051**		
Atlassian					
jira					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/1/2020	4.3	The attachment download resource in Atlassian Jira Server and Data Center before 8.5.5, and from 8.6.0 before 8.8.2, and from 8.9.0 before 8.9.1 allows remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability issue attachments with a mixed multipart content type. **CVE ID : CVE-2020-4022**	N/A	A-ATL-JIRA-100820/21
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/1/2020	3.5	The attachment download resource in Atlassian Jira Server and Data Center before 8.5.5, and from 8.6.0 before 8.8.2, and from 8.9.0 before 8.9.1 allows remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability issue attachments with a vnd.wap.xhtml+xml content type. **CVE ID : CVE-2020-4024**	N/A	A-ATL-JIRA-100820/22
Improper Neutralization of Input During Web Page	7/1/2020	3.5	The attachment download resource in Atlassian Jira Server and Data Center The attachment download	N/A	A-ATL-JIRA-100820/23

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			resource in Atlassian Jira Server and Data Center before 8.5.5, and from 8.6.0 before 8.8.2, and from 8.9.0 before 8.9.1 allows remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability issue attachments with a rdf content type. **CVE ID : CVE-2020-4025**		
Incorrect Authorization	7/1/2020	4	The /rest/project-templates/1.0/createshared resource in Atlassian Jira Server and Data Center before version 8.5.5, from 8.6.0 before 8.7.2, and from 8.8.0 before 8.8.1 allows remote attackers to enumerate project names via an improper authorization vulnerability. **CVE ID : CVE-2020-4029**	N/A	A-ATL-JIRA-100820/24
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/1/2020	4.3	The WYSIWYG editor resource in Jira Server and Data Center before version 8.8.2 allows remote attackers to inject arbitrary HTML or JavaScript names via an Cross Site Scripting (XSS) vulnerability by pasting javascript code into the editor field. **CVE ID : CVE-2020-14164**	N/A	A-ATL-JIRA-100820/25
Incorrect	7/1/2020	5	The	N/A	A-ATL-JIRA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authorization			UniversalAvatarResource.getAvatars resource in Jira Server and Data Center before version 8.9.0 allows remote attackers to obtain information about custom project avatars names via an Improper authorization vulnerability. **CVE ID : CVE-2020-14165**		100820/26
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/1/2020	3.5	The /servicedesk/customer/portals resource in Jira Service Desk Server and Data Center before version 4.10.0 allows remote attackers with project administrator privileges to inject arbitrary HTML or JavaScript names via an Cross Site Scripting (XSS) vulnerability by uploading a html file. **CVE ID : CVE-2020-14166**	N/A	A-ATL-JIRA-100820/27
N/A	7/1/2020	5	The MessageBundleResource resource in Jira Server and Data Center before version 7.13.4, from 8.5.0 before 8.5.5, from 8.8.0 before 8.8.2, and from 8.9.0 before 8.9.1 allows remote attackers to impact the application's availability via an Denial of Service (DoS) vulnerability. **CVE ID : CVE-2020-14167**	N/A	A-ATL-JIRA-100820/28
Information Exposure	7/1/2020	4.3	The email client in Jira Server and Data Center	N/A	A-ATL-JIRA-100820/29

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before version 7.13.16, from 8.5.0 before 8.5.7, from 8.8.0 before 8.8.2, and from 8.9.0 before 8.9.1 allows remote attackers to access outgoing emails between a Jira instance and the SMTP server via man-in-the-middle (MITM) vulnerability. **CVE ID : CVE-2020-14168**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/1/2020	4.3	The quick search component in Atlassian Jira Server and Data Center before 8.9.1 allows remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability **CVE ID : CVE-2020-14169**	N/A	A-ATL-JIRA-100820/30
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	7/3/2020	7.5	This issue exists to document that a security improvement in the way that Jira Server and Data Center use velocity templates has been implemented. The way in which velocity templates were used in Atlassian Jira Server and Data Center in affected versions allowed remote attackers to achieve remote code execution via insecure deserialization, if they were able to exploit a server side template injection vulnerability. The affected versions are	N/A	A-ATL-JIRA-100820/31

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before version 7.13.0, from version 8.0.0 before 8.5.0, and from version 8.6.0 before version 8.8.1. **CVE ID : CVE-2020-14172**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/3/2020	3.5	The file upload feature in Atlassian Jira Server and Data Center in affected versions allows remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability. The affected versions are before version 8.5.4, from version 8.6.0 before 8.6.2, and from version 8.7.0 before 8.7.1. **CVE ID : CVE-2020-14173**	N/A	A-ATL-JIRA-100820/32
Improper Input Validation	7/13/2020	4	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to view titles of a private project via an Insecure Direct Object References (IDOR) vulnerability in the Administration Permission Helper. The affected versions are before version 7.13.6, from version 8.0.0 before 8.5.7, from version 8.6.0 before 8.9.2, and from version 8.10.0 before 8.10.1. **CVE ID : CVE-2020-14174**	N/A	A-ATL-JIRA-100820/33
confluence					
Improper Neutralization	7/1/2020	6.5	Atlassian Confluence Server and Data Center	N/A	A-ATL-CONF-100820/34

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Special Elements in Output Used by a Downstream Component ('Injection')			before version 7.5.1 allowed remote attackers with system administration permissions to bypass velocity template injection mitigations via an injection vulnerability in custom user macros. **CVE ID : CVE-2020-4027**		
bitbucket					
Server-Side Request Forgery (SSRF)	7/9/2020	4	Webhooks in Atlassian Bitbucket Server from version 5.4.0 before version 7.3.1 allow remote attackers to access the content of internal network resources via a Server-Side Request Forgery (SSRF) vulnerability. **CVE ID : CVE-2020-14170**	N/A	A-ATL-BITB-100820/35
Cleartext Transmission of Sensitive Information	7/9/2020	5.8	Atlassian Bitbucket Server from version 4.9.0 before version 7.2.4 allows remote attackers to intercept unencrypted repository import requests via a Man-in-the-Middle (MITM) attack. **CVE ID : CVE-2020-14171**	N/A	A-ATL-BITB-100820/36
jira_software_data_center					
Improper Neutralization of Input During Web Page Generation ('Cross-site	7/1/2020	4.3	The attachment download resource in Atlassian Jira Server and Data Center before 8.5.5, and from 8.6.0 before 8.8.2, and from 8.9.0 before 8.9.1 allows remote attackers to	N/A	A-ATL-JIRA-100820/37

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability issue attachments with a mixed multipart content type. **CVE ID : CVE-2020-4022**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/1/2020	3.5	The attachment download resource in Atlassian Jira Server and Data Center before 8.5.5, and from 8.6.0 before 8.8.2, and from 8.9.0 before 8.9.1 allows remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability issue attachments with a vnd.wap.xhtml+xml content type. **CVE ID : CVE-2020-4024**	N/A	A-ATL-JIRA-100820/38
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/1/2020	3.5	The attachment download resource in Atlassian Jira Server and Data Center The attachment download resource in Atlassian Jira Server and Data Center before 8.5.5, and from 8.6.0 before 8.8.2, and from 8.9.0 before 8.9.1 allows remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability issue attachments with a rdf content type. **CVE ID : CVE-2020-4025**	N/A	A-ATL-JIRA-100820/39

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	7/1/2020	4	The /rest/project-templates/1.0/createshared resource in Atlassian Jira Server and Data Center before version 8.5.5, from 8.6.0 before 8.7.2, and from 8.8.0 before 8.8.1 allows remote attackers to enumerate project names via an improper authorization vulnerability. **CVE ID : CVE-2020-4029**	N/A	A-ATL-JIRA-100820/40
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/1/2020	4.3	The WYSIWYG editor resource in Jira Server and Data Center before version 8.8.2 allows remote attackers to inject arbitrary HTML or JavaScript names via an Cross Site Scripting (XSS) vulnerability by pasting javascript code into the editor field. **CVE ID : CVE-2020-14164**	N/A	A-ATL-JIRA-100820/41
Incorrect Authorization	7/1/2020	5	The UniversalAvatarResource.getAvatars resource in Jira Server and Data Center before version 8.9.0 allows remote attackers to obtain information about custom project avatars names via an Improper authorization vulnerability. **CVE ID : CVE-2020-14165**	N/A	A-ATL-JIRA-100820/42
Improper Neutralization of Input During	7/1/2020	3.5	The /servicedesk/customer/portals resource in Jira	N/A	A-ATL-JIRA-100820/43

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Service Desk Server and Data Center before version 4.10.0 allows remote attackers with project administrator privileges to inject arbitrary HTML or JavaScript names via an Cross Site Scripting (XSS) vulnerability by uploading a html file. **CVE ID : CVE-2020-14166**		
N/A	7/1/2020	5	The MessageBundleResource resource in Jira Server and Data Center before version 7.13.4, from 8.5.0 before 8.5.5, from 8.8.0 before 8.8.2, and from 8.9.0 before 8.9.1 allows remote attackers to impact the application's availability via an Denial of Service (DoS) vulnerability. **CVE ID : CVE-2020-14167**	N/A	A-ATL-JIRA-100820/44
Information Exposure	7/1/2020	4.3	The email client in Jira Server and Data Center before version 7.13.16, from 8.5.0 before 8.5.7, from 8.8.0 before 8.8.2, and from 8.9.0 before 8.9.1 allows remote attackers to access outgoing emails between a Jira instance and the SMTP server via man-in-the-middle (MITM) vulnerability. **CVE ID : CVE-2020-14168**	N/A	A-ATL-JIRA-100820/45
Improper Neutralization	7/1/2020	4.3	The quick search component in Atlassian	N/A	A-ATL-JIRA-100820/46

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input During Web Page Generation ('Cross-site Scripting')			Jira Server and Data Center before 8.9.1 allows remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability **CVE ID : CVE-2020-14169**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	7/3/2020	7.5	This issue exists to document that a security improvement in the way that Jira Server and Data Center use velocity templates has been implemented. The way in which velocity templates were used in Atlassian Jira Server and Data Center in affected versions allowed remote attackers to achieve remote code execution via insecure deserialization, if they were able to exploit a server side template injection vulnerability. The affected versions are before version 7.13.0, from version 8.0.0 before 8.5.0, and from version 8.6.0 before version 8.8.1. **CVE ID : CVE-2020-14172**	N/A	A-ATL-JIRA-100820/47
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/3/2020	3.5	The file upload feature in Atlassian Jira Server and Data Center in affected versions allows remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS)	N/A	A-ATL-JIRA-100820/48

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. The affected versions are before version 8.5.4, from version 8.6.0 before 8.6.2, and from version 8.7.0 before 8.7.1. **CVE ID : CVE-2020-14173**		
Improper Input Validation	7/13/2020	4	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to view titles of a private project via an Insecure Direct Object References (IDOR) vulnerability in the Administration Permission Helper. The affected versions are before version 7.13.6, from version 8.0.0 before 8.5.7, from version 8.6.0 before 8.9.2, and from version 8.10.0 before 8.10.1. **CVE ID : CVE-2020-14174**	N/A	A-ATL-JIRA-100820/49
bareos					
bareos					
Out-of-bounds Write	7/10/2020	6	In Bareos Director less than or equal to 16.2.10, 17.2.9, 18.2.8, and 19.2.7, a heap overflow allows a malicious client to corrupt the director's memory via oversized digest strings sent during initialization of a verify job. Disabling verify jobs mitigates the problem. This issue is also patched in Bareos versions 19.2.8, 18.2.9 and 17.2.10. **CVE ID : CVE-2020-11061**	https://github.com/bareos/bareos/security/advisories/GHSA-mm45-cg35-54j4	A-BAR-BARE-100820/50

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass by Capture-replay	7/10/2020	4.3	Bareos before version 19.2.8 and earlier allows a malicious client to communicate with the director without knowledge of the shared secret if the director allows client initiated connection and connects to the client itself. The malicious client can replay the Bareos director's cram-md5 challenge to the director itself leading to the director responding to the replayed challenge. The response obtained is then a valid reply to the directors original challenge. This is fixed in version 19.2.8. **CVE ID : CVE-2020-4042**	https://github.com/bareos/bareos/security/advisories/GHSA-vqpj-2vhj-h752	A-BAR-BARE-100820/51
Bestsoftinc					
car_rental_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/5/2020	4.3	An issue was discovered in the bestsoftinc Car Rental System plugin through 1.3 for WordPress. Persistent XSS can occur via any of the registration fields. **CVE ID : CVE-2020-15535**	N/A	A-BES-CAR_-100820/52
Checkpoint					
zonealarm_extreme_security					
Improper Privilege Management	7/6/2020	6.5	ZoneAlarm Firewall and Antivirus products before version 15.8.109.18436 allow an attacker who already has access to the system to execute code at	N/A	A-CHE-ZONE-100820/53

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			elevated privileges through a combination of file permission manipulation and exploitation of Windows CVE-2020-00896 on unpatched systems. **CVE ID : CVE-2020-6013**		
Cisco					
digital_network_architecture_center					
Information Exposure	7/2/2020	4	A vulnerability in Cisco Digital Network Architecture (DNA) Center could allow an authenticated, remote attacker to view sensitive information in clear text. The vulnerability is due to insecure storage of certain unencrypted credentials on an affected device. An attacker could exploit this vulnerability by viewing the network device configuration and obtaining credentials that they may not normally have access to. A successful exploit could allow the attacker to use those credentials to discover and manage network devices. **CVE ID : CVE-2020-3391**	N/A	A-CIS-DIGI-100820/54
unified_communications_manager					
Improper Neutralization of Input During Web Page Generation	7/2/2020	4.3	A vulnerability in the web-based management interface of Cisco Unified Communications Manager, Cisco Unified	N/A	A-CIS-UNIF-100820/55

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Communications Manager Session Management Edition, Cisco Unified Communications Manager IM &amp; Presence Service, and Cisco Unity Connection could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information. **CVE ID : CVE-2020-3282**		
unified_communications_manager_im_and_presence_service					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/2/2020	4.3	A vulnerability in the web-based management interface of Cisco Unified Communications Manager, Cisco Unified Communications Manager Session Management Edition, Cisco Unified Communications Manager IM &amp; Presence	N/A	A-CIS-UNIF-100820/56

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service, and Cisco Unity Connection could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information. **CVE ID : CVE-2020-3282**		
identity_services_engine					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/2/2020	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker with administrative credentials to conduct a cross-site scripting (XSS) attack against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input that is	N/A	A-CIS-IDEN-100820/57

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			processed by the web-based management interface. An attacker could exploit these vulnerabilities by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information. To exploit these vulnerabilities, an attacker would need valid administrative credentials. **CVE ID : CVE-2020-3340**		
unity_connection					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/2/2020	4.3	A vulnerability in the web-based management interface of Cisco Unified Communications Manager, Cisco Unified Communications Manager Session Management Edition, Cisco Unified Communications Manager IM &amp; Presence Service, and Cisco Unity Connection could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based	N/A	A-CIS-UNIT-100820/58

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface of the affected software. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information. **CVE ID : CVE-2020-3282**		
unified_customer_voice_portal					
Missing Authentication for Critical Function	7/2/2020	5	A vulnerability in the Java Remote Method Invocation (RMI) interface of Cisco Unified Customer Voice Portal (CVP) could allow an unauthenticated, remote attacker to access sensitive information on an affected device. The vulnerability exists because certain RMI listeners are not properly authenticated. An attacker could exploit this vulnerability by sending a crafted request to the affected listener. A successful exploit could allow the attacker to access sensitive information on an affected device. **CVE ID : CVE-2020-3402**	N/A	A-CIS-UNIF-100820/59
Citrix					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
gateway_plug-in_for_linux					
Improper Input Validation	7/10/2020	4	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in limited information disclosure to low privileged users. **CVE ID : CVE-2020-8195**	N/A	A-CIT-GATE-100820/60
Improper Privilege Management	7/10/2020	4.6	Improper access control in Citrix ADC Gateway Linux client versions before 1.0.0.137 results in local privilege escalation to root. **CVE ID : CVE-2020-8199**	N/A	A-CIT-GATE-100820/61
cli_project					
cli					
Information Exposure Through Log Files	7/7/2020	2.1	Versions of the npm CLI prior to 6.14.6 are vulnerable to an information exposure vulnerability through log files. The CLI supports URLs like "<protocol>://[<user>[:<password>]@]<hostname>[:<port>][:][/]<path>". The password value is not redacted and is printed to stdout and also to any generated log files. **CVE ID : CVE-2020-15095**	https://github.com/npm/cli/security/advisories/GHSA-93f3-23rq-pjfp	A-CLI-CLI-100820/62
cmsuno_project					
cmsuno					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	7/7/2020	4.3	An issue was discovered in CMSUno before 1.6.1. uno.php allows CSRF to change the admin password. **CVE ID : CVE-2020-15600**	https://github.com/boiteasite/cmsuno/issues/15	A-CMS-CMSU-100820/63
code42					
code42					
Improper Privilege Management	7/7/2020	6.5	Code42 environments with on-premises server versions 7.0.4 and earlier allow for possible remote code execution. When an administrator creates a local (non-SSO) user via a Code42-generated email, the administrator has the option to modify content for the email invitation. If the administrator entered template language code in the subject line, that code could be interpreted by the email generation services, potentially resulting in server-side code injection. **CVE ID : CVE-2020-12736**	https://code42.com/r/support/CVE-2020-12736	A-COD-CODE-100820/64
connectwise					
connectwise_automate					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	7/7/2020	6	A SQLi exists in the probe code of all Connectwise Automate versions before 2020.7 or 2019.12. A SQL Injection in the probe implementation to save data to a custom table exists due to inadequate server side validation. As the code creates dynamic	https://slagle.tech/2020/07/06/cve-2020-15008/	A-CON-CONN-100820/65

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SQL for the insert statement and utilizes the user supplied table name with little validation, the table name can be modified to allow arbitrary update commands to be run. Usage of other SQL injection techniques such as timing attacks, it is possible to perform full data extraction as well. Patched in 2020.7 and in a hotfix for 2019.12. **CVE ID : CVE-2020-15008**		
Dell					
emc_data_protection_advisor					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	7/6/2020	9	Dell EMC Data Protection Advisor 6.4, 6.5 and 18.1 contain an OS command injection vulnerability. A remote authenticated malicious user may exploit this vulnerability to execute arbitrary commands on the affected system. **CVE ID : CVE-2020-5352**	N/A	A-DEL-EMC_-100820/66
emc_isilon_onefs					
Incorrect Permission Assignment for Critical Resource	7/6/2020	6.5	Dell EMC Isilon OneFS versions 8.2.2 and earlier and Dell EMC PowerScale version 9.0.0 contain a file permissions vulnerability. An attacker, with network or local file access, could take advantage of insufficiently applied file permissions or gain	N/A	A-DEL-EMC_-100820/67

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized access to files. **CVE ID : CVE-2020-5371**		
powerprotect_data_manager					
Files or Directories Accessible to External Parties	7/6/2020	4	Dell PowerProtect Data Manager (PPDM) versions prior to 19.4 and Dell PowerProtect X400 versions prior to 3.2 contain an improper authorization vulnerability. A remote authenticated malicious user may download any file from the affected PowerProtect virtual machines. **CVE ID : CVE-2020-5356**	N/A	A-DEL-POWE-100820/68
emc_omimssc_for_sccm					
Missing Authentication for Critical Function	7/14/2020	5	Dell EMC OpenManage Integration for Microsoft System Center (OMIMSSC) for SCCM and SCVMM versions prior to 7.2.1 contain an improper authentication vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability to retrieve the system inventory data of the managed device. **CVE ID : CVE-2020-5373**	N/A	A-DEL-EMC_-100820/69
Use of Hard-coded Credentials	7/14/2020	5	Dell EMC OpenManage Integration for Microsoft System Center (OMIMSSC) for SCCM and SCVMM versions prior to 7.2.1 contain a hard-coded	N/A	A-DEL-EMC_-100820/70

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cryptographic key vulnerability. A remote unauthenticated attacker may exploit this vulnerability to gain access to the appliance data for remotely managed devices. **CVE ID : CVE-2020-5374**		
emc_omimssc_for_scvmm					
Missing Authentication for Critical Function	7/14/2020	5	Dell EMC OpenManage Integration for Microsoft System Center (OMIMSSC) for SCCM and SCVMM versions prior to 7.2.1 contain an improper authentication vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability to retrieve the system inventory data of the managed device. **CVE ID : CVE-2020-5373**	N/A	A-DEL-EMC_-100820/71
Use of Hard-coded Credentials	7/14/2020	5	Dell EMC OpenManage Integration for Microsoft System Center (OMIMSSC) for SCCM and SCVMM versions prior to 7.2.1 contain a hard-coded cryptographic key vulnerability. A remote unauthenticated attacker may exploit this vulnerability to gain access to the appliance data for remotely managed devices. **CVE ID : CVE-2020-5374**	N/A	A-DEL-EMC_-100820/72
devcert_project					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
devcert					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	7/10/2020	7.5	A command injection vulnerability in the `devcert` module may lead to remote code execution when users of the module pass untrusted input to the `certificateFor` function. **CVE ID : CVE-2020-8186**	N/A	A-DEV-DEVC-100820/73
django_two-factor_authentication_project					
django_two-factor_authentication					
Cleartext Storage of Sensitive Information	7/10/2020	3.6	Django Two-Factor Authentication before 1.12, stores the user's password in clear text in the user session (base64-encoded). The password is stored in the session when the user submits their username and password, and is removed once they complete authentication by entering a two-factor authentication code. This means that the password is stored in clear text in the session for an arbitrary amount of time, and potentially forever if the user begins the login process by entering their username and password and then leaves before entering their two-factor authentication code. The severity of this issue depends on which type of session storage you have configured: in the worst case, if you're using	https://github.com/Bouke/django-two-factor-auth/security/advisories/GHSA-vhr6-pvjm-9qwf	A-DJA-DJAN-100820/74

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Django's default database session storage, then users' passwords are stored in clear text in your database. In the best case, if you're using Django's signed cookie session, then users' passwords are only stored in clear text within their browser's cookie store. In the common case of using Django's cache session store, the users' passwords are stored in clear text in whatever cache storage you have configured (typically Memcached or Redis). This has been fixed in 1.12. After upgrading, users should be sure to delete any clear text passwords that have been stored. For example, if you're using the database session backend, you'll likely want to delete any session record from the database and purge that data from any database backups or replicas. In addition, affected organizations who have suffered a database breach while using an affected version should inform their users that their clear text passwords have been compromised. All organizations should encourage users whose passwords were insecurely		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			stored to change these passwords on any sites where they were used. As a workaround, wwitching Django's session storage to use signed cookies instead of the database or cache lessens the impact of this issue, but should not be done without a thorough understanding of the security tradeoffs of using signed cookies rather than a server-side session storage. There is no way to fully mitigate the issue without upgrading. **CVE ID : CVE-2020-15105**		
Docker					
docker					
Improper Check for Dropped Privileges	7/13/2020	4.6	The version of docker as released for Red Hat Enterprise Linux 7 Extras via RHBA-2020:0053 advisory included an incorrect version of runc missing the fix for CVE-2019-5736, which was previously fixed via RHSA-2019:0304. This issue could allow a malicious or compromised container to compromise the container host and other containers running on the same host. This issue only affects docker version 1.13.1-108.git4ef4b30.el7, shipped in Red Hat Enterprise Linux 7 Extras.	https://access.redhat.com/errata/RHBA-2020:0427, https://access.redhat.com/security/cve/CVE-2020-14298, https://access.redhat.com/security/vulnerabilities/runcescape, https://bugzilla.redhat.com/show_	A-DOC-DOCK-100820/75

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Both earlier and later versions are not affected. **CVE ID : CVE-2020-14298**	bug.cgi?id=CVE-2019-5736	
Improper Check for Dropped Privileges	7/13/2020	4.6	The docker packages version docker-1.13.1-108.git4ef4b30.el7 as released for Red Hat Enterprise Linux 7 Extras via RHBA-2020:0053 (https://access.redhat.com/errata/RHBA-2020:0053) included an incorrect version of runc that was missing multiple bug and security fixes. One of the fixes regressed in that update was the fix for CVE-2016-9962, that was previously corrected in the docker packages in Red Hat Enterprise Linux 7 Extras via RHSA-2017:0116 (https://access.redhat.com/errata/RHSA-2017:0116). The CVE-2020-14300 was assigned to this security regression and it is specific to the docker packages produced by Red Hat. The original issue - CVE-2016-9962 - could possibly allow a process inside container to compromise a process entering container namespace and execute arbitrary code outside of the container. This could lead to compromise of the container host or other containers running on the	https://access.redhat.com/errata/RHBA-2020:0427, https://access.redhat.com/security/cve/CVE-2016-9962, https://access.redhat.com/security/vulnerabilities/cve-2016-9962, https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2016-9962	A-DOC-DOCK-100820/76

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			same container host. This issue only affects a single version of Docker, 1.13.1-108.git4ef4b30, shipped in Red Hat Enterprise Linux 7. Both earlier and later versions are not affected. **CVE ID : CVE-2020-14300**		
dogtagpki					
dogtagpki					
Improper Certificate Validation	7/14/2020	4	In Dogtag PKI through 10.8.3, the pki.client.PKIConnection class did not enable python-requests certificate validation. Since the verify parameter was hard-coded in all request functions, it was not possible to override the setting. As a result, tools making use of this class, such as the pki-server command, may have been vulnerable to Person-in-the-Middle attacks in certain non-localhost use cases. This is fixed in 10.9.0-b1. **CVE ID : CVE-2020-15720**	N/A	A-DOG-DOGT-100820/77
dronecode					
micro_air_vehicle_link					
Missing Encryption of Sensitive Data	7/3/2020	5	This vulnerability applies to the Micro Air Vehicle Link (MAVLink) protocol and allows a remote attacker to gain access to sensitive information provided it has access to the communication	https://docs.google.com/document/d/1XtbD0ORNkhZ8eKrsbSIZNLyg9sFRXMXbsR2mp37KbI	A-DRO-MICR-100820/78

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			medium. MAVLink is a header-based protocol that does not perform encryption to improve transfer (and reception speed) and efficiency by design. The increasing popularity of the protocol (used accross different autopilots) has led to its use in wired and wireless mediums through insecure communication channels exposing sensitive information to a remote attacker with ability to intercept network traffic. **CVE ID : CVE-2020-10281**	g/edit	
Missing Authentication for Critical Function	7/3/2020	7.5	The Micro Air Vehicle Link (MAVLink) protocol presents no authentication mechanism on its version 1.0 (nor authorization) whichs leads to a variety of attacks including identity spoofing, unauthorized access, PITM attacks and more. According to literature, version 2.0 optionally allows for package signing which mitigates this flaw. Another source mentions that MAVLink 2.0 only provides a simple authentication system based on HMAC. This implies that the flying system overall should add the same symmetric key into all devices of network.	https://github.com/rligocki/Diploma_thesis_px4	A-DRO-MICR-100820/79

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			If not the case, this may cause a security issue, that if one of the devices and its symmetric key are compromised, the whole authentication system is not reliable. **CVE ID : CVE-2020-10282**		
duckduckgo					
duckduckgo					
Information Exposure	7/2/2020	5	** DISPUTED ** The DuckDuckGo application through 5.58.0 for Android, and through 7.47.1.0 for iOS, sends hostnames of visited web sites within HTTPS .ico requests to servers in the duckduckgo.com domain, which might make visit data available temporarily at a Potentially Unwanted Endpoint. NOTE: the vendor has stated "the favicon service adheres to our strict privacy policy." **CVE ID : CVE-2020-15502**	N/A	A-DUC-DUCK-100820/80
electronjs					
electron					
Files or Directories Accessible to External Parties	7/7/2020	2.1	In Electron before versions 7.2.4, 8.2.4, and 9.0.0-beta21, arbitrary local file read is possible by defining unsafe window options on a child window opened via window.open. As a workaround, ensure you are calling `event.preventDefault()`	https://github.com/electron/electron/security/advisories/GHSA-f9mq-jph6-9mhm	A-ELE-ELEC-100820/81

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on all new-window events where the `url` or `options` is not something you expect. This is fixed in versions 9.0.0-beta.21, 8.2.4 and 7.2.4. **CVE ID : CVE-2020-4075**		
N/A	7/7/2020	3.6	In Electron before versions 7.2.4, 8.2.4, and 9.0.0-beta21, there is a context isolation bypass. Code running in the main world context in the renderer can reach into the isolated Electron context and perform privileged actions. Apps using contextIsolation are affected. This is fixed in versions 9.0.0-beta.21, 8.2.4 and 7.2.4. **CVE ID : CVE-2020-4076**	https://github.com/electron/electron/security/advisories/GHSA-m93v-9qjc-3g79	A-ELE-ELEC-100820/82
N/A	7/7/2020	6.5	In Electron before versions 7.2.4, 8.2.4, and 9.0.0-beta21, there is a context isolation bypass. Code running in the main world context in the renderer can reach into the isolated Electron context and perform privileged actions. Apps using both `contextIsolation` and `contextBridge` are affected. This is fixed in versions 9.0.0-beta.21, 8.2.4 and 7.2.4. **CVE ID : CVE-2020-4077**	https://github.com/electron/electron/security/advisories/GHSA-h9jc-284h-533g	A-ELE-ELEC-100820/83
N/A	7/7/2020	4	In Electron before versions	https://gith	A-ELE-ELEC-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			6.1.1, 7.2.4, 8.2.4, and 9.0.0-beta21, there is a context isolation bypass, meaning that code running in the main world context in the renderer can reach into the isolated Electron context and perform privileged actions. Apps using "contextIsolation" are affected. There are no app-side workarounds, you must update your Electron version to be protected. This is fixed in versions 6.1.1, 7.2.4, 8.2.4, and 9.0.0-beta21. **CVE ID : CVE-2020-15096**	ub.com/electron/electron/security/advisories/GHSA-6vrv-94jv-crrg	100820/84
Embedthis					
appweb					
NULL Pointer Dereference	7/13/2020	5	Appweb before 7.2.2 and 8.x before 8.1.0, when built with CGI support, mishandles an HTTP request with a Range header that lacks an exact range. This may result in a NULL pointer dereference and cause a denial of service. **CVE ID : CVE-2020-15689**	https://github.com/embedthis/appweb-gpl/issues/2	A-EMB-APPW-100820/85
envoyproxy					
envoy					
Uncontrolled Resource Consumption	7/1/2020	5	Envoy version 1.14.2, 1.13.2, 1.12.4 or earlier may consume excessive amounts of memory when proxying HTTP/2 requests or responses with many	https://github.com/envoyproxy/envoy/security/advisories/GHSA-	A-ENV-ENVO-100820/86

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			small (i.e. 1 byte) data frames. **CVE ID : CVE-2020-12603**	pc38-4q6c-85p6	
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/1/2020	5	Envoy version 1.14.2, 1.13.2, 1.12.4 or earlier is susceptible to increased memory usage in the case where an HTTP/2 client requests a large payload but does not send enough window updates to consume the entire stream and does not reset the stream. **CVE ID : CVE-2020-12604**	https://github.com/envoyproxy/envoy/security/advisories/GHSA-8hf8-8gvw-ggvx	A-ENV-ENVO-100820/87
Uncontrolled Resource Consumption	7/1/2020	5	Envoy version 1.14.2, 1.13.2, 1.12.4 or earlier may consume excessive amounts of memory when processing HTTP/1.1 headers with long field names or requests with long URLs. **CVE ID : CVE-2020-12605**	https://github.com/envoyproxy/envoy/security/advisories/GHSA-fjxc-jj43-f777	A-ENV-ENVO-100820/88
Origin Validation Error	7/14/2020	5.5	In Envoy before versions 1.12.6, 1.13.4, 1.14.4, and 1.15.0 when validating TLS certificates, Envoy would incorrectly allow a wildcard DNS Subject Alternative Name apply to multiple subdomains. For example, with a SAN of *.example.com, Envoy would incorrectly allow nested.subdomain.example.com, when it should only allow subdomain.example.com.	https://github.com/envoyproxy/envoy/security/advisories/GHSA-w5f5-6qhq-hhrg	A-ENV-ENVO-100820/89

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This defect applies to both validating a client TLS certificate in mTLS, and validating a server TLS certificate for upstream connections. This vulnerability is only applicable to situations where an untrusted entity can obtain a signed wildcard TLS certificate for a domain of which you only intend to trust a subdomain of. For example, if you intend to trust api.mysubdomain.example.com, and an untrusted actor can obtain a signed TLS certificate for *.example.com or *.com. Configurations are vulnerable if they use verify_subject_alt_name in any Envoy version, or if they use match_subject_alt_names in version 1.14 or later. This issue has been fixed in Envoy versions 1.12.6, 1.13.4, 1.14.4, 1.15.0. **CVE ID : CVE-2020-15104**		
Uncontrolled Resource Consumption	7/1/2020	5	Envoy version 1.14.2, 1.13.2, 1.12.4 or earlier may exhaust file descriptors and/or memory when accepting too many connections. **CVE ID : CVE-2020-8663**	https://github.com/envoyproxy/envoy/security/advisories/GHSA-v8q7-fq78-4997	A-ENV-ENVO-100820/90

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
F5					
nginx_controller					
Weak Password Recovery Mechanism for Forgotten Password	7/1/2020	4.6	In NGINX Controller 3.0.0-3.4.0, recovery code required to change a user's password is transmitted and stored in the database in plain text, which allows an attacker who can intercept the database connection or have read access to the database, to request a password reset using the email address of another registered user then retrieve the recovery code. **CVE ID : CVE-2020-5899**	N/A	A-F5-NGIN-100820/91
Cross-Site Request Forgery (CSRF)	7/1/2020	6.8	In versions 3.0.0-3.4.0, 2.0.0-2.9.0, and 1.0.1, there is insufficient cross-site request forgery (CSRF) protections for the NGINX Controller user interface. **CVE ID : CVE-2020-5900**	N/A	A-F5-NGIN-100820/92
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/1/2020	9.3	In NGINX Controller 3.3.0-3.4.0, undisclosed API endpoints may allow for a reflected Cross Site Scripting (XSS) attack. If the victim user is logged in as admin this could result in a complete compromise of the system. **CVE ID : CVE-2020-5901**	N/A	A-F5-NGIN-100820/93
Improper Certificate Validation	7/2/2020	5.8	In versions 3.0.0-3.5.0, 2.0.0-2.9.0, and 1.0.1, when users run the command displayed in NGINX	N/A	A-F5-NGIN-100820/94

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Controller user interface (UI) to fetch the agent installer, the server TLS certificate is not verified. **CVE ID : CVE-2020-5909**		
Improper Authentication	7/2/2020	5	In versions 3.0.0-3.5.0, 2.0.0-2.9.0, and 1.0.1, the Neural Autonomic Transport System (NATS) messaging services in use by the NGINX Controller do not require any form of authentication, so any successful connection would be authorized. **CVE ID : CVE-2020-5910**	N/A	A-F5-NGIN-100820/95
N/A	7/2/2020	7.5	In versions 3.0.0-3.5.0, 2.0.0-2.9.0, and 1.0.1, the NGINX Controller installer starts the download of Kubernetes packages from an HTTP URL On Debian/Ubuntu system. **CVE ID : CVE-2020-5911**	N/A	A-F5-NGIN-100820/96
big-ip_access_policy_manager					
Improper Control of Generation of Code ('Code Injection')	7/1/2020	10	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages. **CVE ID : CVE-2020-5902**	N/A	A-F5-BIG--100820/97

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/1/2020	4.3	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, a Cross-Site Scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility. **CVE ID : CVE-2020-5903**	N/A	A-F5-BIG--100820/98
Cross-Site Request Forgery (CSRF)	7/1/2020	6.8	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, a cross-site request forgery (CSRF) vulnerability in the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, exists in an undisclosed page. **CVE ID : CVE-2020-5904**	N/A	A-F5-BIG--100820/99
Improper Input Validation	7/1/2020	6	In version 11.6.1-11.6.5.2 of the BIG-IP system Configuration utility Network > WCCP page, the system does not sanitize all user-provided data before display. **CVE ID : CVE-2020-5905**	N/A	A-F5-BIG--100820/100
Incorrect Default Permissions	7/1/2020	5.5	In versions 13.1.0-13.1.3.3, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, the BIG-IP system does not properly enforce the access controls for the scp.blacklist files. This allows Admin and Resource Admin users with Secure Copy (SCP)	N/A	A-F5-BIG--100820/101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protocol access to read and overwrite blacklisted files via SCP. **CVE ID : CVE-2020-5906**		
Improper Privilege Management	7/1/2020	6	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, an authorized user provided with access only to the TMOS Shell (tmsh) may be able to conduct arbitrary file read/writes via the built-in sftp functionality. **CVE ID : CVE-2020-5907**	N/A	A-F5-BIG--100820/102
Information Exposure	7/1/2020	2.1	In versions bundled with BIG-IP APM 12.1.0-12.1.5 and 11.6.1-11.6.5.2, Edge Client for Linux exposes full session ID in the local log files. **CVE ID : CVE-2020-5908**	N/A	A-F5-BIG--100820/103
big-ip_advanced_firewall_manager					
Improper Control of Generation of Code ('Code Injection')	7/1/2020	10	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages. **CVE ID : CVE-2020-5902**	N/A	A-F5-BIG--100820/104
Improper	7/1/2020	4.3	In BIG-IP versions 15.0.0-	N/A	A-F5-BIG--

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, a Cross-Site Scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility. **CVE ID : CVE-2020-5903**		100820/105
Cross-Site Request Forgery (CSRF)	7/1/2020	6.8	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, a cross-site request forgery (CSRF) vulnerability in the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, exists in an undisclosed page. **CVE ID : CVE-2020-5904**	N/A	A-F5-BIG--100820/106
Improper Input Validation	7/1/2020	6	In version 11.6.1-11.6.5.2 of the BIG-IP system Configuration utility Network > WCCP page, the system does not sanitize all user-provided data before display. **CVE ID : CVE-2020-5905**	N/A	A-F5-BIG--100820/107
Incorrect Default Permissions	7/1/2020	5.5	In versions 13.1.0-13.1.3.3, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, the BIG-IP system does not properly enforce the access controls for the scp.blacklist files. This allows Admin and Resource Admin users with Secure Copy (SCP) protocol access to read and	N/A	A-F5-BIG--100820/108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			overwrite blacklisted files via SCP. **CVE ID : CVE-2020-5906**		
Improper Privilege Management	7/1/2020	6	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, an authorized user provided with access only to the TMOS Shell (tmsh) may be able to conduct arbitrary file read/writes via the built-in sftp functionality. **CVE ID : CVE-2020-5907**	N/A	A-F5-BIG--100820/109
big-ip_analytics					
Improper Control of Generation of Code ('Code Injection')	7/1/2020	10	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages. **CVE ID : CVE-2020-5902**	N/A	A-F5-BIG--100820/110
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/1/2020	4.3	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, a Cross-Site Scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility.	N/A	A-F5-BIG--100820/111

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5903		
Cross-Site Request Forgery (CSRF)	7/1/2020	6.8	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, a cross-site request forgery (CSRF) vulnerability in the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, exists in an undisclosed page. **CVE ID : CVE-2020-5904**	N/A	A-F5-BIG--100820/112
Improper Input Validation	7/1/2020	6	In version 11.6.1-11.6.5.2 of the BIG-IP system Configuration utility Network > WCCP page, the system does not sanitize all user-provided data before display. **CVE ID : CVE-2020-5905**	N/A	A-F5-BIG--100820/113
Incorrect Default Permissions	7/1/2020	5.5	In versions 13.1.0-13.1.3.3, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, the BIG-IP system does not properly enforce the access controls for the scp.blacklist files. This allows Admin and Resource Admin users with Secure Copy (SCP) protocol access to read and overwrite blacklisted files via SCP. **CVE ID : CVE-2020-5906**	N/A	A-F5-BIG--100820/114
Improper Privilege Management	7/1/2020	6	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, an authorized	N/A	A-F5-BIG--100820/115

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user provided with access only to the TMOS Shell (tmsh) may be able to conduct arbitrary file read/writes via the built-in sftp functionality. **CVE ID : CVE-2020-5907**		
big-ip_application_acceleration_manager					
Improper Control of Generation of Code ('Code Injection')	7/1/2020	10	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages. **CVE ID : CVE-2020-5902**	N/A	A-F5-BIG--100820/116
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/1/2020	4.3	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, a Cross-Site Scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility. **CVE ID : CVE-2020-5903**	N/A	A-F5-BIG--100820/117
Cross-Site Request Forgery (CSRF)	7/1/2020	6.8	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, a cross-site request forgery (CSRF) vulnerability in the Traffic Management User Interface (TMUI), also	N/A	A-F5-BIG--100820/118

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			referred to as the Configuration utility, exists in an undisclosed page. **CVE ID : CVE-2020-5904**		
Improper Input Validation	7/1/2020	6	In version 11.6.1-11.6.5.2 of the BIG-IP system Configuration utility Network > WCCP page, the system does not sanitize all user-provided data before display. **CVE ID : CVE-2020-5905**	N/A	A-F5-BIG--100820/119
Incorrect Default Permissions	7/1/2020	5.5	In versions 13.1.0-13.1.3.3, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, the BIG-IP system does not properly enforce the access controls for the scp.blacklist files. This allows Admin and Resource Admin users with Secure Copy (SCP) protocol access to read and overwrite blacklisted files via SCP. **CVE ID : CVE-2020-5906**	N/A	A-F5-BIG--100820/120
Improper Privilege Management	7/1/2020	6	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, an authorized user provided with access only to the TMOS Shell (tmsh) may be able to conduct arbitrary file read/writes via the built-in sftp functionality. **CVE ID : CVE-2020-5907**	N/A	A-F5-BIG--100820/121
big-ip_application_security_manager					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	7/1/2020	10	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages. **CVE ID : CVE-2020-5902**	N/A	A-F5-BIG--100820/122
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/1/2020	4.3	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, a Cross-Site Scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility. **CVE ID : CVE-2020-5903**	N/A	A-F5-BIG--100820/123
Cross-Site Request Forgery (CSRF)	7/1/2020	6.8	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, a cross-site request forgery (CSRF) vulnerability in the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, exists in an undisclosed page. **CVE ID : CVE-2020-5904**	N/A	A-F5-BIG--100820/124
Improper Input Validation	7/1/2020	6	In version 11.6.1-11.6.5.2 of the BIG-IP system Configuration utility Network > WCCP page, the	N/A	A-F5-BIG--100820/125

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system does not sanitize all user-provided data before display. **CVE ID : CVE-2020-5905**		
Incorrect Default Permissions	7/1/2020	5.5	In versions 13.1.0-13.1.3.3, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, the BIG-IP system does not properly enforce the access controls for the scp.blacklist files. This allows Admin and Resource Admin users with Secure Copy (SCP) protocol access to read and overwrite blacklisted files via SCP. **CVE ID : CVE-2020-5906**	N/A	A-F5-BIG--100820/126
Improper Privilege Management	7/1/2020	6	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, an authorized user provided with access only to the TMOS Shell (tmsh) may be able to conduct arbitrary file read/writes via the built-in sftp functionality. **CVE ID : CVE-2020-5907**	N/A	A-F5-BIG--100820/127
big-ip_domain_name_system					
Improper Control of Generation of Code ('Code Injection')	7/1/2020	10	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a	N/A	A-F5-BIG--100820/128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Remote Code Execution (RCE) vulnerability in undisclosed pages. **CVE ID : CVE-2020-5902**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/1/2020	4.3	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, a Cross-Site Scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility. **CVE ID : CVE-2020-5903**	N/A	A-F5-BIG--100820/129
Cross-Site Request Forgery (CSRF)	7/1/2020	6.8	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, a cross-site request forgery (CSRF) vulnerability in the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, exists in an undisclosed page. **CVE ID : CVE-2020-5904**	N/A	A-F5-BIG--100820/130
Improper Input Validation	7/1/2020	6	In version 11.6.1-11.6.5.2 of the BIG-IP system Configuration utility Network > WCCP page, the system does not sanitize all user-provided data before display. **CVE ID : CVE-2020-5905**	N/A	A-F5-BIG--100820/131
Incorrect Default Permissions	7/1/2020	5.5	In versions 13.1.0-13.1.3.3, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, the BIG-IP system does not properly enforce the access controls for the	N/A	A-F5-BIG--100820/132

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			scp.blacklist files. This allows Admin and Resource Admin users with Secure Copy (SCP) protocol access to read and overwrite blacklisted files via SCP. **CVE ID : CVE-2020-5906**		
Improper Privilege Management	7/1/2020	6	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, an authorized user provided with access only to the TMOS Shell (tmsh) may be able to conduct arbitrary file read/writes via the built-in sftp functionality. **CVE ID : CVE-2020-5907**	N/A	A-F5-BIG--100820/133
big-ip_fraud_protection_service					
Improper Control of Generation of Code ('Code Injection')	7/1/2020	10	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages. **CVE ID : CVE-2020-5902**	N/A	A-F5-BIG--100820/134
Improper Neutralization of Input During Web Page Generation	7/1/2020	4.3	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, a Cross-Site Scripting (XSS)	N/A	A-F5-BIG--100820/135

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			vulnerability exists in an undisclosed page of the BIG-IP Configuration utility. **CVE ID : CVE-2020-5903**		
Cross-Site Request Forgery (CSRF)	7/1/2020	6.8	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, a cross-site request forgery (CSRF) vulnerability in the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, exists in an undisclosed page. **CVE ID : CVE-2020-5904**	N/A	A-F5-BIG--100820/136
Improper Input Validation	7/1/2020	6	In version 11.6.1-11.6.5.2 of the BIG-IP system Configuration utility Network > WCCP page, the system does not sanitize all user-provided data before display. **CVE ID : CVE-2020-5905**	N/A	A-F5-BIG--100820/137
Incorrect Default Permissions	7/1/2020	5.5	In versions 13.1.0-13.1.3.3, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, the BIG-IP system does not properly enforce the access controls for the scp.blacklist files. This allows Admin and Resource Admin users with Secure Copy (SCP) protocol access to read and overwrite blacklisted files via SCP. **CVE ID : CVE-2020-5906**	N/A	A-F5-BIG--100820/138

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	7/1/2020	6	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, an authorized user provided with access only to the TMOS Shell (tmsh) may be able to conduct arbitrary file read/writes via the built-in sftp functionality. **CVE ID : CVE-2020-5907**	N/A	A-F5-BIG--100820/139
big-ip_global_traffic_manager					
Improper Control of Generation of Code ('Code Injection')	7/1/2020	10	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages. **CVE ID : CVE-2020-5902**	N/A	A-F5-BIG--100820/140
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/1/2020	4.3	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, a Cross-Site Scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility. **CVE ID : CVE-2020-5903**	N/A	A-F5-BIG--100820/141
Cross-Site Request Forgery (CSRF)	7/1/2020	6.8	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-	N/A	A-F5-BIG--100820/142

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12.1.5.1, a cross-site request forgery (CSRF) vulnerability in the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, exists in an undisclosed page. **CVE ID : CVE-2020-5904**		
Improper Input Validation	7/1/2020	6	In version 11.6.1-11.6.5.2 of the BIG-IP system Configuration utility Network > WCCP page, the system does not sanitize all user-provided data before display. **CVE ID : CVE-2020-5905**	N/A	A-F5-BIG--100820/143
Incorrect Default Permissions	7/1/2020	5.5	In versions 13.1.0-13.1.3.3, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, the BIG-IP system does not properly enforce the access controls for the scp.blacklist files. This allows Admin and Resource Admin users with Secure Copy (SCP) protocol access to read and overwrite blacklisted files via SCP. **CVE ID : CVE-2020-5906**	N/A	A-F5-BIG--100820/144
Improper Privilege Management	7/1/2020	6	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, an authorized user provided with access only to the TMOS Shell (tmsh) may be able to conduct arbitrary file	N/A	A-F5-BIG--100820/145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			read/writes via the built-in sftp functionality. **CVE ID : CVE-2020-5907**		
big-ip_link_controller					
Improper Control of Generation of Code ('Code Injection')	7/1/2020	10	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages. **CVE ID : CVE-2020-5902**	N/A	A-F5-BIG--100820/146
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/1/2020	4.3	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, a Cross-Site Scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility. **CVE ID : CVE-2020-5903**	N/A	A-F5-BIG--100820/147
Cross-Site Request Forgery (CSRF)	7/1/2020	6.8	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, a cross-site request forgery (CSRF) vulnerability in the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, exists in an undisclosed page.	N/A	A-F5-BIG--100820/148

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5904		
Improper Input Validation	7/1/2020	6	In version 11.6.1-11.6.5.2 of the BIG-IP system Configuration utility Network > WCCP page, the system does not sanitize all user-provided data before display. **CVE ID : CVE-2020-5905**	N/A	A-F5-BIG--100820/149
Incorrect Default Permissions	7/1/2020	5.5	In versions 13.1.0-13.1.3.3, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, the BIG-IP system does not properly enforce the access controls for the scp.blacklist files. This allows Admin and Resource Admin users with Secure Copy (SCP) protocol access to read and overwrite blacklisted files via SCP. **CVE ID : CVE-2020-5906**	N/A	A-F5-BIG--100820/150
Improper Privilege Management	7/1/2020	6	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, an authorized user provided with access only to the TMOS Shell (tmsh) may be able to conduct arbitrary file read/writes via the built-in sftp functionality. **CVE ID : CVE-2020-5907**	N/A	A-F5-BIG--100820/151
big-ip_local_traffic_manager					
Improper Control of Generation of Code ('Code	7/1/2020	10	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-	N/A	A-F5-BIG--100820/152

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			11.6.5.1, the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages. **CVE ID : CVE-2020-5902**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/1/2020	4.3	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, a Cross-Site Scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility. **CVE ID : CVE-2020-5903**	N/A	A-F5-BIG--100820/153
Cross-Site Request Forgery (CSRF)	7/1/2020	6.8	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, a cross-site request forgery (CSRF) vulnerability in the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, exists in an undisclosed page. **CVE ID : CVE-2020-5904**	N/A	A-F5-BIG--100820/154
Improper Input Validation	7/1/2020	6	In version 11.6.1-11.6.5.2 of the BIG-IP system Configuration utility Network > WCCP page, the system does not sanitize all user-provided data before display. **CVE ID : CVE-2020-5905**	N/A	A-F5-BIG--100820/155

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	7/1/2020	5.5	In versions 13.1.0-13.1.3.3, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, the BIG-IP system does not properly enforce the access controls for the scp.blacklist files. This allows Admin and Resource Admin users with Secure Copy (SCP) protocol access to read and overwrite blacklisted files via SCP. **CVE ID : CVE-2020-5906**	N/A	A-F5-BIG--100820/156
Improper Privilege Management	7/1/2020	6	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, an authorized user provided with access only to the TMOS Shell (tmsh) may be able to conduct arbitrary file read/writes via the built-in sftp functionality. **CVE ID : CVE-2020-5907**	N/A	A-F5-BIG--100820/157
big-ip_policy_enforcement_manager					
Improper Control of Generation of Code ('Code Injection')	7/1/2020	10	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages. **CVE ID : CVE-2020-5902**	N/A	A-F5-BIG--100820/158

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/1/2020	4.3	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, a Cross-Site Scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility. **CVE ID : CVE-2020-5903**	N/A	A-F5-BIG--100820/159
Cross-Site Request Forgery (CSRF)	7/1/2020	6.8	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, a cross-site request forgery (CSRF) vulnerability in the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, exists in an undisclosed page. **CVE ID : CVE-2020-5904**	N/A	A-F5-BIG--100820/160
Improper Input Validation	7/1/2020	6	In version 11.6.1-11.6.5.2 of the BIG-IP system Configuration utility Network > WCCP page, the system does not sanitize all user-provided data before display. **CVE ID : CVE-2020-5905**	N/A	A-F5-BIG--100820/161
Incorrect Default Permissions	7/1/2020	5.5	In versions 13.1.0-13.1.3.3, 12.1.0-12.1.5.2, and 11.6.1-11.6.5.2, the BIG-IP system does not properly enforce the access controls for the scp.blacklist files. This allows Admin and Resource Admin users with Secure Copy (SCP)	N/A	A-F5-BIG--100820/162

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protocol access to read and overwrite blacklisted files via SCP. **CVE ID : CVE-2020-5906**		
Improper Privilege Management	7/1/2020	6	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, an authorized user provided with access only to the TMOS Shell (tmsh) may be able to conduct arbitrary file read/writes via the built-in sftp functionality. **CVE ID : CVE-2020-5907**	N/A	A-F5-BIG--100820/163
ssl_orchestrator					
Improper Control of Generation of Code ('Code Injection')	7/1/2020	10	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages. **CVE ID : CVE-2020-5902**	N/A	A-F5-SSL_-100820/164
big-ip_advanced_web_application_firewall					
Improper Control of Generation of Code ('Code Injection')	7/1/2020	10	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, the Traffic Management User Interface (TMUI), also referred to as the	N/A	A-F5-BIG--100820/165

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages. **CVE ID : CVE-2020-5902**		
big-ip_ddos_hybrid_defender					
Improper Control of Generation of Code ('Code Injection')	7/1/2020	10	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages. **CVE ID : CVE-2020-5902**	N/A	A-F5-BIG--100820/166
faceted_search_project					
faceted_search					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/7/2020	3.5	The ke_search (aka Faceted Search) extension through 2.8.2, and 3.x through 3.1.3, for TYPO3 allows XSS. **CVE ID : CVE-2020-15517**	https://typo3.org/security/advisory/typo3-ext-sa-2020-009	A-FAC-FACE-100820/167
ffjpeg_project					
ffjpeg					
Out-of-bounds Write	7/1/2020	4.3	ffjpeg through 2020-02-24 has a heap-based buffer overflow in jfif_decode in jfif.c. **CVE ID : CVE-2020-15470**	N/A	A-FFJ-FFJP-100820/168
github_flavored_markdown_project					
github_flavored_markdown					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	7/1/2020	4	The table extension in GitHub Flavored Markdown before version 0.29.0.gfm.1 takes O(n * n) time to parse certain inputs. An attacker could craft a markdown table which would take an unreasonably long time to process, causing a denial of service. This issue does not affect the upstream cmark project. The issue has been fixed in version 0.29.0.gfm.1. **CVE ID : CVE-2020-5238**	https://github.com/github/cmark-gfm/security/advisories/GHSA-7gc6-9qr5-hc85	A-GIT-GITH-100820/169
Gitlab					
gitlab					
Improper Privilege Management	7/7/2020	5	GitLab EE 11.3 through 13.1.2 has Incorrect Access Control because of the Maven package upload endpoint. **CVE ID : CVE-2020-15525**	https://about.gitlab.com/releases/2020/07/06/critical-security-release-gitlab-13-1-3-released/	A-GIT-GITL-100820/170
gog					
galaxy					
Improper Privilege Management	7/14/2020	7.2	In GOG Galaxy 1.2.67, there is a service that is vulnerable to weak file/service permissions: GalaxyClientService.exe. An attacker can put malicious code in a Trojan horse GalaxyClientService.exe. After that, the attacker can	N/A	A-GOG-GALA-100820/171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			re-start this service as an unprivileged user to escalate his/her privileges and run commands on the machine with SYSTEM rights. **CVE ID : CVE-2020-11827**		
Improper Privilege Management	7/5/2020	9.3	An issue was discovered in GOG Galaxy Client 2.0.17. Local escalation of privileges is possible when a user starts or uninstalls a game because of weak file permissions and missing file integrity checks. **CVE ID : CVE-2020-15528**	N/A	A-GOG-GALA-100820/172
Improper Privilege Management	7/5/2020	9.3	An issue was discovered in GOG Galaxy Client 2.0.17. Local escalation of privileges is possible when a user installs a game or performs a verify/repair operation. The issue exists because of weak file permissions and can be exploited by using opportunistic locks. **CVE ID : CVE-2020-15529**	N/A	A-GOG-GALA-100820/173
Google					
oauth_client_library_for_java					
Missing Authorization	7/9/2020	6.4	PKCE support is not implemented in accordance with the RFC for OAuth 2.0 for Native Apps. Without the use of PKCE, the authorization code returned by an authorization server is not enough to guarantee that	N/A	A-GOO-OAUT-100820/174

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the client that issued the initial authorization request is the one that will be authorized. An attacker is able to obtain the authorization code using a malicious app on the client-side and use it to gain authorization to the protected resource. This affects the package com.google.oauth-client:google-oauth-client before 1.31.0. **CVE ID : CVE-2020-7692**		
hcltechsw					
hcl_verse					
Improper Control of Dynamically-Managed Code Resources	7/15/2020	2.1	"HCL Verse for Android was found to employ dynamic code loading. This mechanism allows a developer to specify which components of the application should not be loaded by default when the application is started. Typically, core components and additional dependencies are loaded natively at runtime; however, dynamically loaded components are only loaded as they are specifically requested. While this can have a positive impact on performance, or grant additional functionality (for example, a non-invasive update feature), it	N/A	A-HCL-HCL_-100820/175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can also open the application to loading unintended code if not implemented properly." **CVE ID : CVE-2020-4100**		
HP					
icewall_sso_dfw					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/8/2020	4.3	A security vulnerability in HPE IceWall SSO Dfw and Dgfw (Domain Gateway Option) could be exploited remotely to cause a remote cross-site scripting (XSS). HPE has provided the following information to resolve this vulnerability in HPE IceWall SSO DFW and Dgfw: https://www.hpe.com/jp/icewall_patchaccess **CVE ID : CVE-2020-7140**	N/A	A-HP-ICEW-100820/176
icewall_sso_dgfw					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/8/2020	4.3	A security vulnerability in HPE IceWall SSO Dfw and Dgfw (Domain Gateway Option) could be exploited remotely to cause a remote cross-site scripting (XSS). HPE has provided the following information to resolve this vulnerability in HPE IceWall SSO DFW and Dgfw: https://www.hpe.com/jp/icewall_patchaccess **CVE ID : CVE-2020-7140**	N/A	A-HP-ICEW-100820/177
Huawei					
hisuite					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Untrusted Search Path	7/6/2020	4.4	Earlier than HiSuite 10.1.0.500 have a DLL hijacking vulnerability. This vulnerability exists due to some DLL file is loaded by HiSuite improperly. And it allows an attacker to load this DLL file of the attacker's choosing. **CVE ID : CVE-2020-9100**	N/A	A-HUA-HISU-100820/178
IBM					
mq_for_hpe_nonstop					
N/A	7/1/2020	4	IBM MQ, IBM MQ Appliance, IBM MQ for HPE NonStop 8.0.4 and 8.1.0 could allow an attacker to cause a denial of service caused by an error within the pubsub logic. IBM X-Force ID: 179081. **CVE ID : CVE-2020-4376**	https://www.ibm.com/support/pages/node/6242364	A-IBM-MQ_F-100820/179
db2					
Uncontrolled Resource Consumption	7/1/2020	5	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 is vulnerable to a denial of service, caused by improper handling of Secure Sockets Layer (SSL) renegotiation requests. By sending specially-crafted requests, a remote attacker could exploit this vulnerability to increase the resource usage on the system. IBM X-Force ID: 178507.	https://www.ibm.com/support/pages/node/6242350	A-IBM-DB2-100820/180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-4355		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/1/2020	7.2	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 is vulnerable to a buffer overflow, caused by improper bounds checking which could allow a local attacker to execute arbitrary code on the system with root privileges. IBM X-Force ID: 178960. **CVE ID : CVE-2020-4363**	https://www.ibm.com/support/pages/node/6242332	A-IBM-DB2-100820/181
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	7/1/2020	1.9	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a local user to obtain sensitive information using a race condition of a symbolic link. IBM X-Force ID: 179268. **CVE ID : CVE-2020-4386**	https://www.ibm.com/support/pages/node/6242342	A-IBM-DB2-100820/182
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	7/1/2020	1.9	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a local user to obtain sensitive information using a race condition of a symbolic link. IBM X-Force ID: 179269. **CVE ID : CVE-2020-4387**	https://www.ibm.com/support/pages/node/6242336	A-IBM-DB2-100820/183
Incorrect Permission	7/1/2020	3.6	IBM DB2 for Linux, UNIX and Windows (includes	https://www.ibm.com/	A-IBM-DB2-100820/184

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assignment for Critical Resource			DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a local attacker to perform unauthorized actions on the system, caused by improper usage of shared memory. By sending a specially-crafted request, an attacker could exploit this vulnerability to obtain sensitive information or cause a denial of service. IBM X-Force ID: 179989. **CVE ID : CVE-2020-4414**	support/pages/node/6242356	
Improper Resource Shutdown or Release	7/1/2020	5	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow an unauthenticated attacker to cause a denial of service due a hang in the execution of a terminate command. IBM X-Force ID: 180076. **CVE ID : CVE-2020-4420**	https://www.ibm.com/support/pages/node/6242362	A-IBM-DB2-100820/185
infosphere_information_server					
Deserialization of Untrusted Data	7/9/2020	9.3	IBM InfoSphere Information Server 11.3, 11.5, and 11.7 could allow a remote attacker to execute arbitrary code on the system, caused by the deserialization of untrusted data. By persuading a victim to visit a specially crafted Web site, an attacker could exploit this vulnerability to execute arbitrary code on	https://www.ibm.com/support/pages/node/6244664	A-IBM-INFO-100820/186

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the system. IBM X-Force ID: 176677. **CVE ID : CVE-2020-4305**		
infosphere_information_server_on_cloud					
Deserialization of Untrusted Data	7/9/2020	9.3	IBM InfoSphere Information Server 11.3, 11.5, and 11.7 could allow a remote attacker to execute arbitrary code on the system, caused by the deserialization of untrusted data. By persuading a victim to visit a specially crafted Web site, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 176677. **CVE ID : CVE-2020-4305**	https://www.ibm.com/support/pages/node/6244664	A-IBM-INFO-100820/187
qradar_security_information_and_event_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/14/2020	3.5	IBM QRadar SIEM 7.3 and 7.4 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: 178961. **CVE ID : CVE-2020-4364**	https://www.ibm.com/support/pages/node/6246139	A-IBM-QRAD-100820/188
Improper Restriction of XML External Entity Reference	7/14/2020	5.5	IBM QRadar SIEM 7.3 and 7.4 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A	https://www.ibm.com/support/pages/node/6	A-IBM-QRAD-100820/189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('XXE')			remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 182365. **CVE ID : CVE-2020-4510**	246133	
N/A	7/14/2020	4	IBM QRadar SIEM 7.3 and 7.4 could allow an authenticated user to cause a denial of service of the qflow process by sending a malformed sflow command. IBM X-Force ID: 182366. **CVE ID : CVE-2020-4511**	https://www.ibm.com/support/pages/node/6246135	A-IBM-QRAD-100820/190
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	7/14/2020	6.5	IBM QRadar SIEM 7.3 and 7.4 could allow a remote privileged user to execute commands. **CVE ID : CVE-2020-4512**	https://www.ibm.com/support/pages/node/6246229	A-IBM-QRAD-100820/191
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/14/2020	4.3	IBM QRadar SIEM 7.3 and 7.4 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: 182368. **CVE ID : CVE-2020-4513**	https://www.ibm.com/support/pages/node/6246131	A-IBM-QRAD-100820/192
security_guardium_insights					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	7/9/2020	4.3	IBM Guardium Activity Insights 10.6 and 11.0 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 174682. **CVE ID : CVE-2020-4173**	https://www.ibm.com/support/pages/node/6244924	A-IBM-SECU-100820/193
infosphere_guardium_activity_monitor					
N/A	7/9/2020	4.3	IBM Guardium Activity Insights 10.6 and 11.0 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 174682. **CVE ID : CVE-2020-4173**	https://www.ibm.com/support/pages/node/6244924	A-IBM-INFO-100820/194
icehrm					
icehrm					
Improper Neutralization	7/10/2020	6.5	An exploitable SQL injection vulnerability	N/A	A-ICE-ICEH-100820/195

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Special Elements used in an SQL Command ('SQL Injection')			exists in the Admin Reports functionality of Glacies IceHRM v26.6.0.OS (Commit bb274de1751ffb9d09482fd2538f9950a94c510a) . A specially crafted HTTP request can cause SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability. **CVE ID : CVE-2020-6114**		
Icewarp					
mail_server					
Exposure of Resource to Wrong Sphere	7/15/2020	4	IceWarp Email Server 12.3.0.1 has Incorrect Access Control for user accounts. **CVE ID : CVE-2020-14064**	N/A	A-ICE-MAIL-100820/196
Unrestricted Upload of File with Dangerous Type	7/15/2020	4	IceWarp Email Server 12.3.0.1 allows remote attackers to upload files and consume disk space. **CVE ID : CVE-2020-14065**	N/A	A-ICE-MAIL-100820/197
Unrestricted Upload of File with Dangerous Type	7/15/2020	6.5	IceWarp Email Server 12.3.0.1 allows remote attackers to upload JavaScript files that are dangerous for clients to access. **CVE ID : CVE-2020-14066**	N/A	A-ICE-MAIL-100820/198
inetsoftware					
i-net_clear_reports					
Improper Restriction of XML External	7/15/2020	7.5	XXE injection can occur in i-net Clear Reports 2019 19.0.287 (Designer), as	https://www.inetsoftware.de/docu	A-INE-I-NE-100820/199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Entity Reference ('XXE')			used in i-net HelpDesk and other products, when XML input containing a reference to an external entity is processed by a weakly configured XML parser. **CVE ID : CVE-2020-12684**	mentation/clear-reports/release-notes/releases/changes_20.4	
ipear_project					
ipear					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	7/14/2020	5.5	In iPear, the manual execution of the eval() function can lead to command injection. Only PCs where commands are manually executed via "For Developers" are affected. This function allows executing any PHP code within iPear which may change, damage, or steal data (files) from the PC. **CVE ID : CVE-2020-11084**	https://github.com/yaBobJonez/iPear/security/advisories/GHSA-4xvp-35fx-hjjj	A-IPE-IPEA-100820/200
Ithemes					
paypal_pro					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	7/2/2020	7.5	The CodePeople Payment Form for PayPal Pro plugin before 1.1.65 for WordPress allows SQL Injection. **CVE ID : CVE-2020-14092**	N/A	A-ITH-PAYP-100820/201
Jenkins					
fortify_on_demand					
Missing Authorization	7/2/2020	4	A missing permission check in Jenkins Fortify on Demand Plugin 6.0.0 and	https://jenkins.io/security/advisor	A-JEN-FORT-100820/202

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier in form-related methods allowed users with Overall/Read access to enumerate credentials ID of credentials stored in Jenkins. **CVE ID : CVE-2020-2202**	y/2020-07-02/#SECURITY-1690	
Cross-Site Request Forgery (CSRF)	7/2/2020	4.3	A cross-site request forgery vulnerability in Jenkins Fortify on Demand Plugin 5.0.1 and earlier allows attackers to connect to the globally configured Fortify on Demand endpoint using attacker-specified credentials IDs. **CVE ID : CVE-2020-2203**	https://jenkins.io/security/advisory/2020-07-02/#SECURITY-1691	A-JEN-FORT-100820/203
Missing Authorization	7/2/2020	5.5	A missing permission check in Jenkins Fortify on Demand Plugin 5.0.1 and earlier allows attackers with Overall/Read permission to connect to the globally configured Fortify on Demand endpoint using attacker-specified credentials IDs. **CVE ID : CVE-2020-2204**	https://jenkins.io/security/advisory/2020-07-02/#SECURITY-1691	A-JEN-FORT-100820/204
kubernetes_ci					
Deserialization of Untrusted Data	7/2/2020	6.5	Jenkins ElasticBox Jenkins Kubernetes CI/CD Plugin 1.3 and earlier does not configure its YAML parser to prevent the instantiation of arbitrary types, resulting in a remote code execution vulnerability.	https://jenkins.io/security/advisory/2020-07-02/#SECURITY-1738	A-JEN-KUBE-100820/205

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-2211		
jenkins					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/15/2020	3.5	Jenkins 2.244 and earlier, LTS 2.235.1 and earlier does not escape the agent name in the build time trend page, resulting in a stored cross-site scripting vulnerability. **CVE ID : CVE-2020-2220**	https://jenkins.io/security/advisory/2020-07-15/#SECURITY-1868	A-JEN-JENK-100820/206
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/15/2020	3.5	Jenkins 2.244 and earlier, LTS 2.235.1 and earlier does not escape the upstream job's display name shown as part of a build cause, resulting in a stored cross-site scripting vulnerability. **CVE ID : CVE-2020-2221**	https://jenkins.io/security/advisory/2020-07-15/#SECURITY-1901	A-JEN-JENK-100820/207
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/15/2020	3.5	Jenkins 2.244 and earlier, LTS 2.235.1 and earlier does not escape the job name in the 'Keep this build forever' badge tooltip, resulting in a stored cross-site scripting vulnerability. **CVE ID : CVE-2020-2222**	https://jenkins.io/security/advisory/2020-07-15/#SECURITY-1902	A-JEN-JENK-100820/208
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/15/2020	3.5	Jenkins 2.244 and earlier, LTS 2.235.1 and earlier does not escape correctly the 'href' attribute of links to downstream jobs displayed in the build console page, resulting in a stored cross-site scripting vulnerability. **CVE ID : CVE-2020-2223**	https://jenkins.io/security/advisory/2020-07-15/#SECURITY-1945	A-JEN-JENK-100820/209

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
matrix_project					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/15/2020	3.5	Jenkins Matrix Project Plugin 1.16 and earlier does not escape the node names shown in tooltips on the overview page of builds with a single axis, resulting in a stored cross-site scripting vulnerability. **CVE ID : CVE-2020-2224**	https://jenkins.io/security/advisory/2020-07-15/#SECURITY-1924	A-JEN-MATR-100820/210
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/15/2020	3.5	Jenkins Matrix Project Plugin 1.16 and earlier does not escape the axis names shown in tooltips on the overview page of builds with multiple axes, resulting in a stored cross-site scripting vulnerability. **CVE ID : CVE-2020-2225**	https://jenkins.io/security/advisory/2020-07-15/#SECURITY-1925	A-JEN-MATR-100820/211
zephyr_for_jira_test_management					
Cross-Site Request Forgery (CSRF)	7/2/2020	4.3	A cross-site request forgery vulnerability in Jenkins Zephyr for JIRA Test Management Plugin 1.5 and earlier allows attackers to connect to an attacker-specified HTTP server using attacker-specified username and password. **CVE ID : CVE-2020-2215**	https://jenkins.io/security/advisory/2020-07-02/#SECURITY-1762	A-JEN-ZEPH-100820/212
Missing Authorization	7/2/2020	4	A missing permission check in Jenkins Zephyr for JIRA Test Management Plugin 1.5 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified HTTP server	https://jenkins.io/security/advisory/2020-07-02/#SECURITY-1762	A-JEN-ZEPH-100820/213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			using attacker-specified username and password. **CVE ID : CVE-2020-2216**		
sonargraph_integration					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/2/2020	3.5	Jenkins Sonargraph Integration Plugin 3.0.0 and earlier does not escape the file path for the Log file field form validation, resulting in a stored cross-site scripting vulnerability. **CVE ID : CVE-2020-2201**	https://jenkins.io/security/advisory/2020-07-02/#SECURITY-1775	A-JEN-SONA-100820/214
vncrecorder					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/2/2020	3.5	Jenkins VncRecorder Plugin 1.25 and earlier does not escape a tool path in the `checkVncServ` form validation endpoint, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by Jenkins administrators. **CVE ID : CVE-2020-2205**	https://jenkins.io/security/advisory/2020-07-02/#SECURITY-1728%20(1)	A-JEN-VNCR-100820/215
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/2/2020	4.3	Jenkins VncRecorder Plugin 1.25 and earlier does not escape a parameter value in the checkVncServ form validation endpoint, resulting in a reflected cross-site scripting (XSS) vulnerability. **CVE ID : CVE-2020-2206**	https://jenkins.io/security/advisory/2020-07-02/#SECURITY-1728%20(2)	A-JEN-VNCR-100820/216
matrix_authorization_strategy					
Improper Neutralization of Input During Web Page	7/15/2020	3.5	Jenkins Matrix Authorization Strategy Plugin 2.6.1 and earlier does not escape user	https://jenkins.io/security/advisory/2020-07-	A-JEN-MATR-100820/217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			names shown in the configuration, resulting in a stored cross-site scripting vulnerability. **CVE ID : CVE-2020-2226**	15/#SECURITY-1909	
deployer_framework					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/15/2020	3.5	Jenkins Deployer Framework Plugin 1.2 and earlier does not escape the URL displayed in the build home page, resulting in a stored cross-site scripting vulnerability. **CVE ID : CVE-2020-2227**	https://jenkins.io/security/advisory/2020-07-15/#SECURITY-1915	A-JEN-DEPL-100820/218
gitlab_authentication					
Improper Privilege Management	7/15/2020	6.5	Jenkins Gitlab Authentication Plugin 1.5 and earlier does not perform group authorization checks properly, resulting in a privilege escalation vulnerability. **CVE ID : CVE-2020-2228**	https://jenkins.io/security/advisory/2020-07-15/#SECURITY-1792	A-JEN-GITL-100820/219
vncviewer					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/2/2020	4.3	Jenkins VncViewer Plugin 1.7 and earlier does not escape a parameter value in the checkVncServ form validation endpoint, resulting in a reflected cross-site scripting (XSS) vulnerability. **CVE ID : CVE-2020-2207**	https://jenkins.io/security/advisory/2020-07-02/#SECURITY-1776	A-JEN-VNCV-100820/220
slack_upload					
Insufficiently Protected	7/2/2020	4	Jenkins Slack Upload Plugin 1.7 and earlier	https://jenkins.io/secu	A-JEN-SLAC-100820/221

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			stores a secret unencrypted in job config.xml files on the Jenkins master where it can be viewed by users with Extended Read permission, or access to the master file system. **CVE ID : CVE-2020-2208**	rity/advisory/2020-07-02/#SECURITY-1627	
testcomplete_support					
Insufficiently Protected Credentials	7/2/2020	4	Jenkins TestComplete support Plugin 2.4.1 and earlier stores a password unencrypted in job config.xml files on the Jenkins master where it can be viewed by users with Extended Read permission, or access to the master file system. **CVE ID : CVE-2020-2209**	https://jenkins.io/security/advisory/2020-07-02/#SECURITY-1686	A-JEN-TEST-100820/222
stash_branch_parameter					
Cleartext Transmission of Sensitive Information	7/2/2020	4.3	Jenkins Stash Branch Parameter Plugin 0.3.0 and earlier transmits configured passwords in plain text as part of its global Jenkins configuration form, potentially resulting in their exposure. **CVE ID : CVE-2020-2210**	https://jenkins.io/security/advisory/2020-07-02/#SECURITY-1656	A-JEN-STAS-100820/223
github_coverage_reporter					
Insufficiently Protected Credentials	7/2/2020	4	Jenkins GitHub Coverage Reporter Plugin 1.8 and earlier stores secrets unencrypted in its global configuration file on the	https://jenkins.io/security/advisory/2020-07-02/#SECUR	A-JEN-GITH-100820/224

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Jenkins master where they can be viewed by users with access to the master file system or read permissions on the system configuration. **CVE ID : CVE-2020-2212**	ITY-1632	
white_source					
Insufficiently Protected Credentials	7/2/2020	4	Jenkins White Source Plugin 19.1.1 and earlier stores credentials unencrypted in its global configuration file and in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission (config.xml), or access to the master file system. **CVE ID : CVE-2020-2213**	https://jenkins.io/security/advisory/2020-07-02/#SECURITY-1630	A-JEN-WHIT-100820/225
zap_pipeline					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/2/2020	3.5	Jenkins ZAP Pipeline Plugin 1.9 and earlier programmatically disables Content-Security-Policy protection for user-generated content in workspaces, archived artifacts, etc. that Jenkins offers for download. **CVE ID : CVE-2020-2214**	https://jenkins.io/security/advisory/2020-07-02/#SECURITY-1811	A-JEN-ZAP_-100820/226
link_column					
Improper Neutralization of Input During Web Page Generation	7/2/2020	3.5	Jenkins Link Column Plugin 1.0 and earlier does not filter URLs of links created by users with View/Configure	https://jenkins.io/security/advisory/2020-07-02/#SECUR	A-JEN-LINK-100820/227

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			permission, resulting in a stored cross-site scripting vulnerability. **CVE ID : CVE-2020-2219**	ITY-1803	
jh_captcha_project					
jh_captcha					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/7/2020	3.5	The jh_captcha extension through 2.1.3, and 3.x through 3.0.2, for TYPO3 allows XSS. **CVE ID : CVE-2020-15514**	https://typo3.org/security/advisory/typo3-ext-sa-2020-012	A-JH_-JH_C-100820/228
jison_project					
jison					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	7/15/2020	10	Insufficient input validation in npm package `jison` <= 0.4.18 may lead to OS command injection attacks. **CVE ID : CVE-2020-8178**	N/A	A-JIS-JISO-100820/229
Joomla					
joomla\!					
Cross-Site Request Forgery (CSRF)	7/15/2020	6.8	An issue was discovered in Joomla! through 3.9.19. A missing token check in the remove request section of com_privacy causes a CSRF vulnerability. **CVE ID : CVE-2020-15695**	N/A	A-JOO-JOOM-100820/230
Improper Neutralization of Input During Web Page Generation	7/15/2020	4.3	An issue was discovered in Joomla! through 3.9.19. Lack of input filtering and escaping allows XSS attacks in	N/A	A-JOO-JOOM-100820/231

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			mod_random_image. **CVE ID : CVE-2020-15696**		
Incorrect Permission Assignment for Critical Resource	7/15/2020	4	An issue was discovered in Joomla! through 3.9.19. Internal read-only fields in the User table class could be modified by users. **CVE ID : CVE-2020-15697**	N/A	A-JOO-JOOM-100820/232
Information Exposure	7/15/2020	5	An issue was discovered in Joomla! through 3.9.19. Inadequate filtering on the system information screen could expose Redis or proxy credentials **CVE ID : CVE-2020-15698**	N/A	A-JOO-JOOM-100820/233
Insufficient Verification of Data Authenticity	7/15/2020	5	An issue was discovered in Joomla! through 3.9.19. Missing validation checks on the usergroups table object can result in a broken site configuration. **CVE ID : CVE-2020-15699**	N/A	A-JOO-JOOM-100820/234
Cross-Site Request Forgery (CSRF)	7/15/2020	6.8	An issue was discovered in Joomla! through 3.9.19. A missing token check in the ajax_install endpoint of com_installer causes a CSRF vulnerability. **CVE ID : CVE-2020-15700**	N/A	A-JOO-JOOM-100820/235
journal-theme					
journal					
Information Exposure	7/1/2020	5	The Journal theme before 3.1.0 for OpenCart allows exposure of sensitive data via SQL errors. **CVE ID : CVE-2020-15478**	N/A	A-JOU-JOUR-100820/236

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
king-theme					
kingcomposer					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/9/2020	4.3	A reflected Cross-Site Scripting (XSS) Vulnerability in the KingComposer plugin through 2.9.4 for WordPress allows remote attackers to trick a victim into submitting an install_online_preset AJAX request containing base64-encoded JavaScript (in the kc-online-preset-data POST parameter) that is executed in the victim's browser. **CVE ID : CVE-2020-15299**	N/A	A-KIN-KING-100820/237
Kronos					
web_time_and_attendance					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	7/15/2020	4	A Blind SQL Injection vulnerability in Kronos WebTA 3.8.x and later before 4.0 (affecting the com.threeis.webta.H352premPayRequest servlet's SortBy parameter) allows an attacker with the Employee, Supervisor, or Timekeeper role to read sensitive data from the database. **CVE ID : CVE-2020-14982**	N/A	A-KRO-WEB_-100820/238
Leadtools					
leadtools					
Out-of-bounds Write	7/1/2020	6.8	An exploitable code execution vulnerability exists in the ANI file format	N/A	A-LEA-LEAD-100820/239

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parser of Leadtools 20. A specially crafted ANI file can cause a buffer overflow resulting in remote code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2020-6089**		
ledger					
ledger_live					
Insufficient Verification of Data Authenticity	7/2/2020	5.8	Ledger Live before 2.7.0 does not handle Bitcoin's Replace-By-Fee (RBF). It increases the user's balance with the value of an unconfirmed transaction as soon as it is received (before the transaction is confirmed) and does not decrease the balance when it is canceled. As a result, users are exposed to basic double spending attacks, amplified double spending attacks, and DoS attacks without user consent. **CVE ID : CVE-2020-12119**	https://donjon.ledger.com/lsb/012/	A-LED-LEDG-100820/240
Libraw					
libraw					
Improper Input Validation	7/2/2020	5	LibRaw before 0.20-RC1 lacks a thumbnail size range check. This affects decoders/unpack_thumb.cpp, postprocessing/mem_image.cpp, and utils/thumb_utils.cpp. For	N/A	A-LIB-LIBR-100820/241

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			example, malloc(sizeof(libraw_processed_image_t)+T.tlength) occurs without validating T.tlength. **CVE ID : CVE-2020-15503**		
librehealth					
librehealth_ehr					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/15/2020	6	LibreHealth EMR v2.0.0 is vulnerable to XSS that results in the ability to force arbitrary actions on behalf of other users including administrators. **CVE ID : CVE-2020-11436**	N/A	A-LIB-LIBR-100820/242
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	7/15/2020	4	LibreHealth EMR v2.0.0 is affected by SQL injection allowing low-privilege authenticated users to enumerate the database. **CVE ID : CVE-2020-11437**	N/A	A-LIB-LIBR-100820/243
Cross-Site Request Forgery (CSRF)	7/15/2020	6.8	LibreHealth EMR v2.0.0 is affected by systemic CSRF. **CVE ID : CVE-2020-11438**	N/A	A-LIB-LIBR-100820/244
Improper Input Validation	7/15/2020	9	LibreHealth EMR v2.0.0 is affected by a Local File Inclusion issue allowing arbitrary PHP to be included and executed within the EMR application. **CVE ID : CVE-2020-11439**	N/A	A-LIB-LIBR-100820/245
libslirp_project					
libslirp					
Out-of-bounds	7/9/2020	2.1	An out-of-bounds read	N/A	A-LIB-LIBS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Read			vulnerability was found in the SLiRP networking implementation of the QEMU emulator. This flaw occurs in the icmp6_send_echoreply() routine while replying to an ICMP echo request, also known as ping. This flaw allows a malicious guest to leak the contents of the host memory, resulting in possible information disclosure. This flaw affects versions of libslirp before 4.3.1. **CVE ID : CVE-2020-10756**		100820/246
Linuxfoundation					
harbor					
Server-Side Request Forgery (SSRF)	7/15/2020	4	Harbor prior to 2.0.1 allows SSRF with this limitation: an attacker with the ability to edit projects can scan ports of hosts accessible on the Harbor server's intranet. **CVE ID : CVE-2020-13788**	https://www.soluble.ai/blog/harbor-ssrf-cve-2020-13788	A-LIN-HARB-100820/247
osquery					
Untrusted Search Path	7/10/2020	4.4	osquery before version 4.4.0 enables a priviledge escalation vulnerability. If a Window system is configured with a PATH that contains a user-writable directory then a local user may write a zlib1.dll DLL, which osquery will attempt to load. Since osquery runs	https://github.com/osquery/osquery/security/advisories/GHSA-2xwp-8fv7-c5pm	A-LIN-OSQU-100820/248

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with elevated privileges this enables local escalation. This is fixed in version 4.4.0. **CVE ID : CVE-2020-11081**		
locutus					
locutus_php					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	7/1/2020	7.5	php/exec/escapeshellarg in Locutus PHP through 2.0.11 allows an attacker to achieve code execution. **CVE ID : CVE-2020-13619**	N/A	A-LOC-LOCU-100820/249
lodash					
lodash					
Allocation of Resources Without Limits or Throttling	7/15/2020	5.8	Prototype pollution attack when using _.zipObjectDeep in lodash <= 4.17.15. **CVE ID : CVE-2020-8203**	https://security.netapp.com/advisory/ntap-20200724-0006/	A-LOD-LODA-100820/250
Mcafee					
web_gateway					
Improper Encoding or Escaping of Output	7/15/2020	4.3	Inappropriate Encoding for output context in McAfee Web Gateway (MWG) prior to 9.2.1 allows remote attacker to cause MWG to return an ambiguous redirect response via getting a user to click on a malicious URL. **CVE ID : CVE-2020-7292**	N/A	A-MCA-WEB_-100820/251
total_protection					
Improper	7/3/2020	1.9	Privilege Escalation	https://ser	A-MCA-TOTA-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			vulnerability in McAfee Total Protection (MTP) prior to 16.0.R26 allows local users to delete files the user would otherwise not have access to via manipulating symbolic links to redirect a McAfee delete action to an unintended file. This is achieved through running a malicious script or program on the target machine. **CVE ID : CVE-2020-7281**	vice.mcafee.com/webcenter/portal/cp/home/articleview?articleId=TS103062	100820/252
Improper Link Resolution Before File Access ('Link Following')	7/3/2020	3.3	Privilege Escalation vulnerability in McAfee Total Protection (MTP) before 16.0.R26 allows local users to delete files the user would otherwise not have access to via manipulating symbolic links to redirect a McAfee delete action to an unintended file. This is achieved through running a malicious script or program on the target machine. **CVE ID : CVE-2020-7282**	https://service.mcafee.com/webcenter/portal/cp/home/articleview?articleId=TS103062	A-MCA-TOTA-100820/253
Improper Privilege Management	7/3/2020	4.6	Privilege Escalation vulnerability in McAfee Total Protection (MTP) before 16.0.R26 allows local users to create and edit files via symbolic link manipulation in a location they would otherwise not have access to. This is	https://service.mcafee.com/webcenter/portal/cp/home/articleview?articleId=TS103062	A-MCA-TOTA-100820/254

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			achieved through running a malicious script or program on the target machine. **CVE ID : CVE-2020-7283**		
network_security_management					
Information Exposure	7/3/2020	7.2	Exposure of Sensitive Information in McAfee Network Security Management (NSM) prior to 10.1.7.7 allows local users to gain unauthorised access to the root account via execution of carefully crafted commands from the restricted command line interface (CLI). **CVE ID : CVE-2020-7284**	N/A	A-MCA-NETW-100820/255
mercari					
mercari					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	7/9/2020	6.8	Android App 'Mercari' (Japan version) prior to version 3.52.0 allows arbitrary method execution of a Java object by a remote attacker via a Man-In-The-Middle attack by using Java Reflection API of JavaScript code on WebView. **CVE ID : CVE-2020-5604**	N/A	A-MER-MERC-100820/256
Microfocus					
identity_manager					
Improper Privilege Management	7/8/2020	7.5	Elevation of privilege and/or unauthorized access vulnerability in Micro Focus Identity Manager. Affecting	N/A	A-MIC-IDEN-100820/257

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 4.7.3 and 4.8.1 hot fix 1. The vulnerability could allow information exposure that can result in an elevation of privilege or an unauthorized access. **CVE ID : CVE-2020-11849**		
Microsoft					
365_apps					
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1240**	N/A	A-MIC-365_-100820/258
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists when Microsoft Office software reads out of bound memory due to an uninitialized variable, which could disclose the contents of memory, aka 'Microsoft Office Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1445. **CVE ID : CVE-2020-1342**	N/A	A-MIC-365_-100820/259
Improper Restriction of Operations within the Bounds of a	7/14/2020	6.8	A remote code execution vulnerability exists in Microsoft Outlook software when it fails to properly handle objects in memory, aka 'Microsoft	N/A	A-MIC-365_-100820/260

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Outlook Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1349**		
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists when Microsoft Office improperly discloses the contents of its memory, aka 'Microsoft Office Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1342. **CVE ID : CVE-2020-1445**	N/A	A-MIC-365_-100820/261
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	6.8	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1447, CVE-2020-1448. **CVE ID : CVE-2020-1446**	N/A	A-MIC-365_-100820/262
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	6.8	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1446, CVE-2020-1448. **CVE ID : CVE-2020-1447**	N/A	A-MIC-365_-100820/263
Origin Validation	7/14/2020	9.3	A remote code execution vulnerability exists in Microsoft Project software	N/A	A-MIC-365_-100820/264

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Error			when the software fails to check the source markup of a file, aka 'Microsoft Project Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1449**		
Untrusted Search Path	7/14/2020	9.3	A remote code execution vulnerability exists when Microsoft Office improperly validates input before loading dynamic link library (DLL) files, aka 'Microsoft Office Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1458**	N/A	A-MIC-365_-100820/265
office_web_apps					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/14/2020	4.3	A spoofing vulnerability exists when an Office Web Apps server does not properly sanitize a specially crafted request, aka 'Office Web Apps XSS Vulnerability'. **CVE ID : CVE-2020-1442**	N/A	A-MIC-OFFI-100820/266
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists when Microsoft Office software reads out of bound memory due to an uninitialized variable, which could disclose the contents of memory, aka 'Microsoft Office Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1445.	N/A	A-MIC-OFFI-100820/267

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1342		
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists when Microsoft Office improperly discloses the contents of its memory, aka 'Microsoft Office Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1342. **CVE ID : CVE-2020-1445**	N/A	A-MIC-OFFI-100820/268
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	6.8	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1447, CVE-2020-1448. **CVE ID : CVE-2020-1446**	N/A	A-MIC-OFFI-100820/269
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	6.8	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1446, CVE-2020-1448. **CVE ID : CVE-2020-1447**	N/A	A-MIC-OFFI-100820/270
Improper Restriction of Operations within the Bounds of a	7/14/2020	6.8	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory,	N/A	A-MIC-OFFI-100820/271

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1446, CVE-2020-1447. **CVE ID : CVE-2020-1448**		
windows_defender					
Improper Privilege Management	7/14/2020	3.6	An elevation of privilege vulnerability exists when the MpSigStub.exe for Defender allows file deletion in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Defender Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1461**	N/A	A-MIC-WIND-100820/272
forefront_endpoint_protection_2010					
Improper Privilege Management	7/14/2020	3.6	An elevation of privilege vulnerability exists when the MpSigStub.exe for Defender allows file deletion in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Defender Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1461**	N/A	A-MIC-FORE-100820/273
system_center_endpoint_protection					
Improper Privilege Management	7/14/2020	3.6	An elevation of privilege vulnerability exists when the MpSigStub.exe for	N/A	A-MIC-SYST-100820/274

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Defender allows file deletion in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Defender Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1461**		
security_essentials					
Improper Privilege Management	7/14/2020	3.6	An elevation of privilege vulnerability exists when the MpSigStub.exe for Defender allows file deletion in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Defender Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1461**	N/A	A-MIC-SECU-100820/275
onedrive					
Improper Privilege Management	7/14/2020	7.2	An elevation of privilege vulnerability exists in Microsoft OneDrive that allows file deletion in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft OneDrive Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1465**	N/A	A-MIC-ONED-100820/276
word_rt					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	6.8	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1447, CVE-2020-1448. **CVE ID : CVE-2020-1446**	N/A	A-MIC-WORD-100820/277
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	6.8	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1446, CVE-2020-1448. **CVE ID : CVE-2020-1447**	N/A	A-MIC-WORD-100820/278
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	6.8	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1446, CVE-2020-1447. **CVE ID : CVE-2020-1448**	N/A	A-MIC-WORD-100820/279
project_2016					
Origin Validation Error	7/14/2020	9.3	A remote code execution vulnerability exists in Microsoft Project software when the software fails to check the source markup	N/A	A-MIC-PROJ-100820/280

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of a file, aka 'Microsoft Project Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1449**		
visual_studio					
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Diagnostics Hub Standard Collector Service fails to properly sanitize input, leading to an unsecure library-loading behavior, aka 'Windows Diagnostics Hub Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1418. **CVE ID : CVE-2020-1393**	N/A	A-MIC-VISU-100820/281
edge					
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists when Microsoft Edge PDF Reader improperly handles objects in memory, aka 'Microsoft Edge PDF Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1433**	N/A	A-MIC-EDGE-100820/282
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists when Skype for Business is accessed via Microsoft Edge (EdgeHTML-based), aka 'Skype for Business via Microsoft Edge (EdgeHTML-based) Information Disclosure	N/A	A-MIC-EDGE-100820/283

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. **CVE ID : CVE-2020-1462**		
office					
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists when Microsoft Office software reads out of bound memory due to an uninitialized variable, which could disclose the contents of memory, aka 'Microsoft Office Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1445. **CVE ID : CVE-2020-1342**	N/A	A-MIC-OFFI-100820/284
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	6.8	A remote code execution vulnerability exists in Microsoft Outlook software when it fails to properly handle objects in memory, aka 'Microsoft Outlook Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1349**	N/A	A-MIC-OFFI-100820/285
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists when Microsoft Office improperly discloses the contents of its memory, aka 'Microsoft Office Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1342. **CVE ID : CVE-2020-1445**	N/A	A-MIC-OFFI-100820/286
Improper	7/14/2020	6.8	A remote code execution	N/A	A-MIC-OFFI-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1447, CVE-2020-1448. **CVE ID : CVE-2020-1446**		100820/287
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	6.8	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1446, CVE-2020-1448. **CVE ID : CVE-2020-1447**	N/A	A-MIC-OFFI-100820/288
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	6.8	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1446, CVE-2020-1447. **CVE ID : CVE-2020-1448**	N/A	A-MIC-OFFI-100820/289
Origin Validation Error	7/14/2020	9.3	A remote code execution vulnerability exists in Microsoft Project software when the software fails to check the source markup of a file, aka 'Microsoft Project Remote Code	N/A	A-MIC-OFFI-100820/290

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability'. **CVE ID : CVE-2020-1449**		
internet_explorer					
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	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'. **CVE ID : CVE-2020-1403**	N/A	A-MIC-INTE-100820/291
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists when Skype for Business is accessed via Internet Explorer, aka 'Skype for Business via Internet Explorer Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1432**	N/A	A-MIC-INTE-100820/292
.net_core					
N/A	7/14/2020	6.8	A remote code execution vulnerability exists in .NET Framework, Microsoft SharePoint, and Visual Studio when the software fails to check the source markup of XML file input, aka '.NET Framework, SharePoint Server, and Visual Studio Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1147**	N/A	A-MIC-.NET-100820/293
.net_framework					
N/A	7/14/2020	6.8	A remote code execution vulnerability exists in .NET Framework, Microsoft SharePoint, and Visual	N/A	A-MIC-.NET-100820/294

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Studio when the software fails to check the source markup of XML file input, aka '.NET Framework, SharePoint Server, and Visual Studio Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1147**		
visual_studio_2017					
N/A	7/14/2020	6.8	A remote code execution vulnerability exists in .NET Framework, Microsoft SharePoint, and Visual Studio when the software fails to check the source markup of XML file input, aka '.NET Framework, SharePoint Server, and Visual Studio Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1147**	N/A	A-MIC-VISU-100820/295
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Diagnostics Hub Standard Collector Service fails to properly sanitize input, leading to an unsecure library-loading behavior, aka 'Windows Diagnostics Hub Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1418. **CVE ID : CVE-2020-1393**	N/A	A-MIC-VISU-100820/296
sharepoint_server					
Improper Neutralization of Special	7/14/2020	3.5	A spoofing vulnerability exists when Microsoft SharePoint Server does not	N/A	A-MIC-SHAR-100820/297

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements in Output Used by a Downstream Component ('Injection')			properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'. **CVE ID : CVE-2020-1443**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/14/2020	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-2020-1450, CVE-2020-1451. **CVE ID : CVE-2020-1456**	N/A	A-MIC-SHAR-100820/298
Improper Privilege Management	7/14/2020	7.5	An elevation of privilege vulnerability exists when Microsoft SharePoint Server and Skype for Business Server improperly handle OAuth token validation, aka 'Microsoft Office Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1025**	N/A	A-MIC-SHAR-100820/299
N/A	7/14/2020	6.8	A remote code execution vulnerability exists in .NET Framework, Microsoft SharePoint, and Visual Studio when the software fails to check the source markup of XML file input, aka '.NET Framework, SharePoint Server, and	N/A	A-MIC-SHAR-100820/300

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Visual Studio Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1147**		
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists when Microsoft Office software reads out of bound memory due to an uninitialized variable, which could disclose the contents of memory, aka 'Microsoft Office Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1445. **CVE ID : CVE-2020-1342**	N/A	A-MIC-SHAR-100820/301
Deserialization of Untrusted Data	7/14/2020	6.5	A remote code execution vulnerability exists in PerformancePoint Services for SharePoint Server when the software fails to check the source markup of XML file input, aka 'PerformancePoint Services Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1439**	N/A	A-MIC-SHAR-100820/302
Improper Input Validation	7/14/2020	4.3	A remote code execution vulnerability exists in the way Microsoft SharePoint software parses specially crafted email messages, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1444**	N/A	A-MIC-SHAR-100820/303
Improper Restriction of	7/14/2020	6.8	A remote code execution vulnerability exists in	N/A	A-MIC-SHAR-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1447, CVE-2020-1448. **CVE ID : CVE-2020-1446**		100820/304
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	6.8	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1446, CVE-2020-1448. **CVE ID : CVE-2020-1447**	N/A	A-MIC-SHAR-100820/305
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	6.8	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1446, CVE-2020-1447. **CVE ID : CVE-2020-1448**	N/A	A-MIC-SHAR-100820/306
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/14/2020	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	N/A	A-MIC-SHAR-100820/307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1451, CVE-2020-1456. **CVE ID : CVE-2020-1450**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/14/2020	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-2020-1450, CVE-2020-1456. **CVE ID : CVE-2020-1451**	N/A	A-MIC-SHAR-100820/308
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/14/2020	3.5	This vulnerability is caused when SharePoint Server does not properly sanitize a specially crafted request to an affected SharePoint server.An authenticated attacker could exploit this vulnerability by sending a specially crafted request to an affected SharePoint server, aka 'Microsoft SharePoint Reflective XSS Vulnerability'. **CVE ID : CVE-2020-1454**	N/A	A-MIC-SHAR-100820/309
outlook					
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	6.8	A remote code execution vulnerability exists in Microsoft Outlook software when it fails to properly handle objects in memory, aka 'Microsoft	N/A	A-MIC-OUTL-100820/310

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Outlook Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1349**		
word					
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists when Microsoft Office software reads out of bound memory due to an uninitialized variable, which could disclose the contents of memory, aka 'Microsoft Office Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1445. **CVE ID : CVE-2020-1342**	N/A	A-MIC-WORD-100820/311
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists when Microsoft Office improperly discloses the contents of its memory, aka 'Microsoft Office Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1342. **CVE ID : CVE-2020-1445**	N/A	A-MIC-WORD-100820/312
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	6.8	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1447, CVE-2020-1448.	N/A	A-MIC-WORD-100820/313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1446		
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	6.8	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1446, CVE-2020-1448. **CVE ID : CVE-2020-1447**	N/A	A-MIC-WORD-100820/314
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	6.8	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1446, CVE-2020-1447. **CVE ID : CVE-2020-1448**	N/A	A-MIC-WORD-100820/315
sharepoint_enterprise_server					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	7/14/2020	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'. **CVE ID : CVE-2020-1443**	N/A	A-MIC-SHAR-100820/316
Improper Neutralization of Input During Web Page Generation	7/14/2020	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted	N/A	A-MIC-SHAR-100820/317

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-1450, CVE-2020-1451. **CVE ID : CVE-2020-1456**		
Improper Privilege Management	7/14/2020	7.5	An elevation of privilege vulnerability exists when Microsoft SharePoint Server and Skype for Business Server improperly handle OAuth token validation, aka 'Microsoft Office Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1025**	N/A	A-MIC-SHAR-100820/318
N/A	7/14/2020	6.8	A remote code execution vulnerability exists in .NET Framework, Microsoft SharePoint, and Visual Studio when the software fails to check the source markup of XML file input, aka '.NET Framework, SharePoint Server, and Visual Studio Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1147**	N/A	A-MIC-SHAR-100820/319
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists when Microsoft Office software reads out of bound memory due to an uninitialized variable, which could disclose the contents of memory, aka 'Microsoft Office	N/A	A-MIC-SHAR-100820/320

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1445. **CVE ID : CVE-2020-1342**		
Deserialization of Untrusted Data	7/14/2020	6.5	A remote code execution vulnerability exists in PerformancePoint Services for SharePoint Server when the software fails to check the source markup of XML file input, aka 'PerformancePoint Services Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1439**	N/A	A-MIC-SHAR-100820/321
Improper Input Validation	7/14/2020	4.3	A remote code execution vulnerability exists in the way Microsoft SharePoint software parses specially crafted email messages, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1444**	N/A	A-MIC-SHAR-100820/322
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists when Microsoft Office improperly discloses the contents of its memory, aka 'Microsoft Office Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1342. **CVE ID : CVE-2020-1445**	N/A	A-MIC-SHAR-100820/323
Improper Restriction of Operations	7/14/2020	6.8	A remote code execution vulnerability exists in Microsoft Word software	N/A	A-MIC-SHAR-100820/324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1447, CVE-2020-1448. **CVE ID : CVE-2020-1446**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	6.8	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1446, CVE-2020-1448. **CVE ID : CVE-2020-1447**	N/A	A-MIC-SHAR-100820/325
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	6.8	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1446, CVE-2020-1447. **CVE ID : CVE-2020-1448**	N/A	A-MIC-SHAR-100820/326
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/14/2020	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	N/A	A-MIC-SHAR-100820/327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. This CVE ID is unique from CVE-2020-1451, CVE-2020-1456. **CVE ID : CVE-2020-1450**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/14/2020	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-2020-1450, CVE-2020-1456. **CVE ID : CVE-2020-1451**	N/A	A-MIC-SHAR-100820/328
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/14/2020	3.5	This vulnerability is caused when SharePoint Server does not properly sanitize a specially crafted request to an affected SharePoint server.An authenticated attacker could exploit this vulnerability by sending a specially crafted request to an affected SharePoint server, aka 'Microsoft SharePoint Reflective XSS Vulnerability'. **CVE ID : CVE-2020-1454**	N/A	A-MIC-SHAR-100820/329
office_online_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/14/2020	4.3	A spoofing vulnerability exists when an Office Web Apps server does not properly sanitize a specially crafted request, aka 'Office Web Apps XSS Vulnerability'.	N/A	A-MIC-OFFI-100820/330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1442		
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists when Microsoft Office software reads out of bound memory due to an uninitialized variable, which could disclose the contents of memory, aka 'Microsoft Office Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1445. **CVE ID : CVE-2020-1342**	N/A	A-MIC-OFFI-100820/331
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists when Microsoft Office improperly discloses the contents of its memory, aka 'Microsoft Office Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1342. **CVE ID : CVE-2020-1445**	N/A	A-MIC-OFFI-100820/332
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	6.8	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1447, CVE-2020-1448. **CVE ID : CVE-2020-1446**	N/A	A-MIC-OFFI-100820/333
Improper Restriction of	7/14/2020	6.8	A remote code execution vulnerability exists in	N/A	A-MIC-OFFI-100820/334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1446, CVE-2020-1448. **CVE ID : CVE-2020-1447**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	6.8	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka 'Microsoft Word Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1446, CVE-2020-1447. **CVE ID : CVE-2020-1448**	N/A	A-MIC-OFFI-100820/335
sharepoint_foundation					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	7/14/2020	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'. **CVE ID : CVE-2020-1443**	N/A	A-MIC-SHAR-100820/336
Improper Privilege Management	7/14/2020	7.5	An elevation of privilege vulnerability exists when Microsoft SharePoint Server and Skype for Business Server improperly handle OAuth token validation, aka 'Microsoft Office Elevation	N/A	A-MIC-SHAR-100820/337

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of Privilege Vulnerability'. **CVE ID : CVE-2020-1025**		
Deserialization of Untrusted Data	7/14/2020	6.5	A remote code execution vulnerability exists in PerformancePoint Services for SharePoint Server when the software fails to check the source markup of XML file input, aka 'PerformancePoint Services Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1439**	N/A	A-MIC-SHAR-100820/338
Improper Input Validation	7/14/2020	4.3	A remote code execution vulnerability exists in the way Microsoft SharePoint software parses specially crafted email messages, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1444**	N/A	A-MIC-SHAR-100820/339
skype_for_business					
Improper Privilege Management	7/14/2020	7.5	An elevation of privilege vulnerability exists when Microsoft SharePoint Server and Skype for Business Server improperly handle OAuth token validation, aka 'Microsoft Office Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1025**	N/A	A-MIC-SKYP-100820/340
visual_studio_2019					
N/A	7/14/2020	6.8	A remote code execution vulnerability exists in .NET Framework, Microsoft SharePoint, and Visual	N/A	A-MIC-VISU-100820/341

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Studio when the software fails to check the source markup of XML file input, aka '.NET Framework, SharePoint Server, and Visual Studio Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1147**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Diagnostics Hub Standard Collector Service fails to properly sanitize input, leading to an unsecure library-loading behavior, aka 'Windows Diagnostics Hub Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1418. **CVE ID : CVE-2020-1393**	N/A	A-MIC-VISU-100820/342
bond					
Unrestricted Upload of File with Dangerous Type	7/14/2020	5	A denial of service vulnerability exists when the .NET implementation of Bond improperly parses input, aka 'Bond Denial of Service Vulnerability'. **CVE ID : CVE-2020-1469**	N/A	A-MIC-BOND-100820/343
visual_studio_code_eslint_extension					
Improper Neutralization of Special Elements in Output Used by a Downstream Component	7/14/2020	9.3	A remote code execution vulnerability exists in the ESLint extension for Visual Studio Code when it validates source code after opening a project, aka 'Visual Studio Code ESLint Extention Remote Code	N/A	A-MIC-VISU-100820/344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Injection')			Execution Vulnerability'. **CVE ID : CVE-2020-1481**		
lync					
Improper Privilege Management	7/14/2020	7.5	An elevation of privilege vulnerability exists when Microsoft SharePoint Server and Skype for Business Server improperly handle OAuth token validation, aka 'Microsoft Office Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1025**	N/A	A-MIC-LYNC-100820/345
milkytracker_project					
milkytracker					
Use After Free	7/6/2020	4.3	PlayerGeneric.cpp in MilkyTracker through 1.02.00 has a use-after-free in the PlayerGeneric destructor. **CVE ID : CVE-2020-15569**	N/A	A-MIL-MILK-100820/346
Misp					
misp					
Cross-Site Request Forgery (CSRF)	7/14/2020	6.8	In MISP before 2.4.129, setting a favourite homepage was not CSRF protected. **CVE ID : CVE-2020-15711**	N/A	A-MIS-MISP-100820/347
mittwald					
typo3_forum					
Incorrect Authorization	7/7/2020	5	The typo3_forum extension before 1.2.1 for TYPO3 has Incorrect Access Control. **CVE ID : CVE-2020-15513**	https://typo3.org/security/advisory/typo3-ext-sa-2020-010	A-MIT-TYPO-100820/348

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mm_forum_project					
mm_forum					
Cross-Site Request Forgery (CSRF)	7/7/2020	5.8	The mm_forum extension through 1.9.5 for TYPO3 allows XSS that can be exploited via CSRF. **CVE ID : CVE-2020-15516**	https://typo3.org/security/advisory/typo3-ext-sa-2020-013	A-MM_-MM_F-100820/349
Mobileiron					
cloud					
N/A	7/7/2020	7.5	A remote code execution vulnerability in MobileIron Core and Connector versions 10.6 and earlier, and Sentry versions 9.8 and earlier that allows remote attackers to execute arbitrary code via unspecified vectors. **CVE ID : CVE-2020-15505**	N/A	A-MOB-CLOU-100820/350
Improper Authentication	7/7/2020	7.5	An Authentication Bypass vulnerability in MobileIron Core and Connector versions 10.6 and earlier that allows remote attackers to bypass authentication mechanisms via unspecified vectors. **CVE ID : CVE-2020-15506**	N/A	A-MOB-CLOU-100820/351
Information Exposure	7/7/2020	5	An arbitrary file reading vulnerability in MobileIron Core and Connector versions 10.6 and earlier that allows remote attackers to read files on the system via unspecified vectors.	N/A	A-MOB-CLOU-100820/352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-15507		
core					
N/A	7/7/2020	7.5	A remote code execution vulnerability in MobileIron Core and Connector versions 10.6 and earlier, and Sentry versions 9.8 and earlier that allows remote attackers to execute arbitrary code via unspecified vectors. **CVE ID : CVE-2020-15505**	N/A	A-MOB-CORE-100820/353
Improper Authentication	7/7/2020	7.5	An Authentication Bypass vulnerability in MobileIron Core and Connector versions 10.6 and earlier that allows remote attackers to bypass authentication mechanisms via unspecified vectors. **CVE ID : CVE-2020-15506**	N/A	A-MOB-CORE-100820/354
Information Exposure	7/7/2020	5	An arbitrary file reading vulnerability in MobileIron Core and Connector versions 10.6 and earlier that allows remote attackers to read files on the system via unspecified vectors. **CVE ID : CVE-2020-15507**	N/A	A-MOB-CORE-100820/355
enterprise_connector					
N/A	7/7/2020	7.5	A remote code execution vulnerability in MobileIron Core and Connector versions 10.6 and earlier, and Sentry versions 9.8 and earlier that allows	N/A	A-MOB-ENTE-100820/356

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers to execute arbitrary code via unspecified vectors. **CVE ID : CVE-2020-15505**		
Improper Authentication	7/7/2020	7.5	An Authentication Bypass vulnerability in MobileIron Core and Connector versions 10.6 and earlier that allows remote attackers to bypass authentication mechanisms via unspecified vectors. **CVE ID : CVE-2020-15506**	N/A	A-MOB-ENTE-100820/357
Information Exposure	7/7/2020	5	An arbitrary file reading vulnerability in MobileIron Core and Connector versions 10.6 and earlier that allows remote attackers to read files on the system via unspecified vectors. **CVE ID : CVE-2020-15507**	N/A	A-MOB-ENTE-100820/358
reporting_database					
N/A	7/7/2020	7.5	A remote code execution vulnerability in MobileIron Core and Connector versions 10.6 and earlier, and Sentry versions 9.8 and earlier that allows remote attackers to execute arbitrary code via unspecified vectors. **CVE ID : CVE-2020-15505**	N/A	A-MOB-REPO-100820/359
Improper Authentication	7/7/2020	7.5	An Authentication Bypass vulnerability in MobileIron Core and Connector versions 10.6 and earlier	N/A	A-MOB-REPO-100820/360

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that allows remote attackers to bypass authentication mechanisms via unspecified vectors. **CVE ID : CVE-2020-15506**		
Information Exposure	7/7/2020	5	An arbitrary file reading vulnerability in MobileIron Core and Connector versions 10.6 and earlier that allows remote attackers to read files on the system via unspecified vectors. **CVE ID : CVE-2020-15507**	N/A	A-MOB-REPO-100820/361
sentry					
N/A	7/7/2020	7.5	A remote code execution vulnerability in MobileIron Core and Connector versions 10.6 and earlier, and Sentry versions 9.8 and earlier that allows remote attackers to execute arbitrary code via unspecified vectors. **CVE ID : CVE-2020-15505**	N/A	A-MOB-SENT-100820/362
Improper Authentication	7/7/2020	7.5	An Authentication Bypass vulnerability in MobileIron Core and Connector versions 10.6 and earlier that allows remote attackers to bypass authentication mechanisms via unspecified vectors. **CVE ID : CVE-2020-15506**	N/A	A-MOB-SENT-100820/363
Information Exposure	7/7/2020	5	An arbitrary file reading vulnerability in MobileIron	N/A	A-MOB-SENT-100820/364

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Core and Connector versions 10.6 and earlier that allows remote attackers to read files on the system via unspecified vectors. **CVE ID : CVE-2020-15507**		
mods-for-hesk					
mods_for_hesk					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/9/2020	4.3	An issue was discovered in Mods for HESK 3.1.0 through 2019.1.0. A Stored XSS issue allows remote unauthenticated attackers to abuse a helpdesk user's logged in session. A user with sufficient privileges to change their login-page image must open a crafted ticket. **CVE ID : CVE-2020-13992**	N/A	A-MOD-MODS-100820/365
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	7/9/2020	5	An issue was discovered in Mods for HESK 3.1.0 through 2019.1.0. A blind time-based SQL injection issue allows remote unauthenticated attackers to retrieve information from the database via a ticket. **CVE ID : CVE-2020-13993**	N/A	A-MOD-MODS-100820/366
Improper Control of Generation of Code ('Code Injection')	7/9/2020	6.5	An issue was discovered in Mods for HESK 3.1.0 through 2019.1.0. A privileged user can achieve code execution on the server via a ticket because of improper access control of uploaded resources.	N/A	A-MOD-MODS-100820/367

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This might be exploitable in conjunction with CVE-2020-13992 by an unauthenticated attacker. **CVE ID : CVE-2020-13994**		
monstaftp					
monsta_ftp					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/1/2020	4.3	Monsta FTP 2.10.1 or below is prone to a stored cross-site scripting vulnerability in the language setting due to insufficient output encoding. **CVE ID : CVE-2020-14055**	N/A	A-MON-MONS-100820/368
Server-Side Request Forgery (SSRF)	7/1/2020	7.5	Monsta FTP 2.10.1 or below is prone to a server-side request forgery vulnerability due to insufficient restriction of the web fetch functionality. This allows attackers to read arbitrary local files and interact with arbitrary third-party services. **CVE ID : CVE-2020-14056**	N/A	A-MON-MONS-100820/369
Externally Controlled Reference to a Resource in Another Sphere	7/1/2020	7.5	Monsta FTP 2.10.1 or below allows external control of paths used in filesystem operations. This allows attackers to read and write arbitrary local files, allowing an attacker to gain remote code execution in common deployments. **CVE ID : CVE-2020-14057**	N/A	A-MON-MONS-100820/370
Mozilla					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
firefox					
Information Exposure Through Discrepancy	7/9/2020	1.2	NSS has shown timing differences when performing DSA signatures, which was exploitable and could eventually leak private keys. This vulnerability affects Thunderbird < 68.9.0, Firefox < 77, and Firefox ESR < 68.9. **CVE ID : CVE-2020-12399**	N/A	A-MOZ-FIRE-100820/371
Use of a Broken or Risky Cryptographic Algorithm	7/9/2020	1.2	During RSA key generation, bignum implementations used a variation of the Binary Extended Euclidean Algorithm which entailed significantly input-dependent flow. This allowed an attacker able to perform electromagnetic-based side channel attacks to record traces leading to the recovery of the secret primes. *Note:* An unmodified Firefox browser does not generate RSA keys in normal operation and is not affected, but products built on top of it might. This vulnerability affects Firefox < 78. **CVE ID : CVE-2020-12402**	N/A	A-MOZ-FIRE-100820/372
Information Exposure	7/9/2020	4.3	For native-to-JS bridging the app requires a unique token to be passed that ensures non-app code can't call the bridging	N/A	A-MOZ-FIRE-100820/373

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			functions. That token could leak when used for downloading files. This vulnerability affects Firefox for iOS < 26. **CVE ID : CVE-2020-12404**		
Use After Free	7/9/2020	2.6	When browsing a malicious page, a race condition in our SharedWorkerService could occur and lead to a potentially exploitable crash. This vulnerability affects Thunderbird < 68.9.0, Firefox < 77, and Firefox ESR < 68.9. **CVE ID : CVE-2020-12405**	N/A	A-MOZ-FIRE-100820/374
Insufficient Verification of Data Authenticity	7/9/2020	9.3	Mozilla Developer Iain Ireland discovered a missing type check during unboxed objects removal, resulting in a crash. We presume that with enough effort that it could be exploited to run arbitrary code. This vulnerability affects Thunderbird < 68.9.0, Firefox < 77, and Firefox ESR < 68.9. **CVE ID : CVE-2020-12406**	N/A	A-MOZ-FIRE-100820/375
Information Exposure	7/9/2020	2.6	Mozilla Developer Nicolas Silva found that when using WebRender, Firefox would under certain conditions leak arbitrary GPU memory to the visible screen. The leaked memory content was visible to the user, but not	N/A	A-MOZ-FIRE-100820/376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			observable from web content. This vulnerability affects Firefox < 77. **CVE ID : CVE-2020-12407**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	7/9/2020	4.3	When browsing a document hosted on an IP address, an attacker could insert certain characters to flip domain and path information in the address bar. This vulnerability affects Firefox < 77. **CVE ID : CVE-2020-12408**	N/A	A-MOZ-FIRE-100820/377
N/A	7/9/2020	6.8	When using certain blank characters in a URL, they where incorrectly rendered as spaces instead of an encoded URL. This vulnerability affects Firefox < 77. **CVE ID : CVE-2020-12409**	N/A	A-MOZ-FIRE-100820/378
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/9/2020	9.3	Mozilla developers reported memory safety bugs present in Firefox 76 and Firefox ESR 68.8. 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 Thunderbird < 68.9.0, Firefox < 77, and Firefox ESR < 68.9. **CVE ID : CVE-2020-12410**	N/A	A-MOZ-FIRE-100820/379
Improper Restriction of	7/9/2020	9.3	Mozilla developers reported memory safety	N/A	A-MOZ-FIRE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer		🟥	bugs present in Firefox 76. 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 < 77. **CVE ID : CVE-2020-12411**		100820/380
N/A	7/9/2020	4.3	By navigating a tab using the history API, an attacker could cause the address bar to display the incorrect domain (with the https:// scheme, a blocked port number such as '1', and without a lock icon) while controlling the page contents. This vulnerability affects Firefox < 70. **CVE ID : CVE-2020-12412**	N/A	A-MOZ-FIRE-100820/381
Incomplete Cleanup	7/9/2020	4.3	IndexedDB should be cleared when leaving private browsing mode and it is not, the API for WKWebViewConfiguration was being used incorrectly and requires the private instance of this object be deleted when leaving private mode. This vulnerability affects Firefox for iOS < 27. **CVE ID : CVE-2020-12414**	N/A	A-MOZ-FIRE-100820/382
Incorrect Default	7/9/2020	4.3	When "%2F" was present in a manifest URL, Firefox's	N/A	A-MOZ-FIRE-100820/383

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Permissions			AppCache behavior may have become confused and allowed a manifest to be served from a subdirectory. This could cause the appcache to be used to service requests for the top level directory. This vulnerability affects Firefox < 78. **CVE ID : CVE-2020-12415**		
Use After Free	7/9/2020	9.3	A VideoStreamEncoder may have been freed in a race condition with VideoBroadcaster::AddOrUpdateSink, resulting in a use-after-free, memory corruption, and a potentially exploitable crash. This vulnerability affects Firefox < 78. **CVE ID : CVE-2020-12416**	N/A	A-MOZ-FIRE-100820/384
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/9/2020	9.3	Due to confusion about ValueTags on JavaScript Objects, an object may pass through the type barrier, resulting in memory corruption and a potentially exploitable crash. *Note: this issue only affects Firefox on ARM64 platforms.* This vulnerability affects Firefox ESR < 68.10, Firefox < 78, and Thunderbird < 68.10.0. **CVE ID : CVE-2020-12417**	N/A	A-MOZ-FIRE-100820/385
Out-of-bounds Read	7/9/2020	4.3	Manipulating individual parts of a URL object could	N/A	A-MOZ-FIRE-100820/386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have caused an out-of-bounds read, leaking process memory to malicious JavaScript. This vulnerability affects Firefox ESR < 68.10, Firefox < 78, and Thunderbird < 68.10.0. **CVE ID : CVE-2020-12418**		
Use After Free	7/9/2020	9.3	When processing callbacks that occurred during window flushing in the parent process, the associated window may die; causing a use-after-free condition. This could have led to memory corruption and a potentially exploitable crash. This vulnerability affects Firefox ESR < 68.10, Firefox < 78, and Thunderbird < 68.10.0. **CVE ID : CVE-2020-12419**	N/A	A-MOZ-FIRE-100820/387
Use After Free	7/9/2020	9.3	When trying to connect to a STUN server, a race condition could have caused a use-after-free of a pointer, leading to memory corruption and a potentially exploitable crash. This vulnerability affects Firefox ESR < 68.10, Firefox < 78, and Thunderbird < 68.10.0. **CVE ID : CVE-2020-12420**	N/A	A-MOZ-FIRE-100820/388
Improper Certificate Validation	7/9/2020	4.3	When performing add-on updates, certificate chains terminating in non-built-	N/A	A-MOZ-FIRE-100820/389

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in-roots were rejected (even if they were legitimately added by an administrator.) This could have caused add-ons to become out-of-date silently without notification to the user. This vulnerability affects Firefox ESR < 68.10, Firefox < 78, and Thunderbird < 68.10.0. **CVE ID : CVE-2020-12421**		
Out-of-bounds Write	7/9/2020	7.6	In non-standard configurations, a JPEG image created by JavaScript could have caused an internal variable to overflow, resulting in an out of bounds write, memory corruption, and a potentially exploitable crash. This vulnerability affects Firefox < 78. **CVE ID : CVE-2020-12422**	N/A	A-MOZ-FIRE-100820/390
Uncontrolled Search Path Element	7/9/2020	6.9	When the Windows DLL "webauthn.dll" was missing from the Operating System, and a malicious one was placed in a folder in the user's %PATH%, Firefox may have loaded the DLL, leading to arbitrary code execution. *Note: This issue only affects the Windows operating system; other operating systems are unaffected.* This vulnerability affects	N/A	A-MOZ-FIRE-100820/391

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Firefox < 78. **CVE ID : CVE-2020-12423**		
Incorrect Default Permissions	7/9/2020	4.3	When constructing a permission prompt for WebRTC, a URI was supplied from the content process. This URI was untrusted, and could have been the URI of an origin that was previously granted permission; bypassing the prompt. This vulnerability affects Firefox < 78. **CVE ID : CVE-2020-12424**	N/A	A-MOZ-FIRE-100820/392
Out-of-bounds Read	7/9/2020	4.3	Due to confusion processing a hyphen character in Date.parse(), a one-byte out of bounds read could have occurred, leading to potential information disclosure. This vulnerability affects Firefox < 78. **CVE ID : CVE-2020-12425**	N/A	A-MOZ-FIRE-100820/393
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/9/2020	9.3	Mozilla developers and community members reported memory safety bugs present in Firefox 77. 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 < 78. **CVE ID : CVE-2020-12426**	N/A	A-MOZ-FIRE-100820/394

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
firefox_esr					
Information Exposure Through Discrepancy	7/9/2020	1.2	NSS has shown timing differences when performing DSA signatures, which was exploitable and could eventually leak private keys. This vulnerability affects Thunderbird < 68.9.0, Firefox < 77, and Firefox ESR < 68.9. **CVE ID : CVE-2020-12399**	N/A	A-MOZ-FIRE-100820/395
Use After Free	7/9/2020	2.6	When browsing a malicious page, a race condition in our SharedWorkerService could occur and lead to a potentially exploitable crash. This vulnerability affects Thunderbird < 68.9.0, Firefox < 77, and Firefox ESR < 68.9. **CVE ID : CVE-2020-12405**	N/A	A-MOZ-FIRE-100820/396
Insufficient Verification of Data Authenticity	7/9/2020	9.3	Mozilla Developer Iain Ireland discovered a missing type check during unboxed objects removal, resulting in a crash. We presume that with enough effort that it could be exploited to run arbitrary code. This vulnerability affects Thunderbird < 68.9.0, Firefox < 77, and Firefox ESR < 68.9. **CVE ID : CVE-2020-12406**	N/A	A-MOZ-FIRE-100820/397
Improper Restriction of Operations	7/9/2020	9.3	Mozilla developers reported memory safety bugs present in Firefox 76	N/A	A-MOZ-FIRE-100820/398

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			and Firefox ESR 68.8. 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 Thunderbird < 68.9.0, Firefox < 77, and Firefox ESR < 68.9. **CVE ID : CVE-2020-12410**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/9/2020	9.3	Due to confusion about ValueTags on JavaScript Objects, an object may pass through the type barrier, resulting in memory corruption and a potentially exploitable crash. *Note: this issue only affects Firefox on ARM64 platforms.* This vulnerability affects Firefox ESR < 68.10, Firefox < 78, and Thunderbird < 68.10.0. **CVE ID : CVE-2020-12417**	N/A	A-MOZ-FIRE-100820/399
Out-of-bounds Read	7/9/2020	4.3	Manipulating individual parts of a URL object could have caused an out-of-bounds read, leaking process memory to malicious JavaScript. This vulnerability affects Firefox ESR < 68.10, Firefox < 78, and Thunderbird < 68.10.0. **CVE ID : CVE-2020-12418**	N/A	A-MOZ-FIRE-100820/400

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	7/9/2020	9.3	When processing callbacks that occurred during window flushing in the parent process, the associated window may die; causing a use-after-free condition. This could have led to memory corruption and a potentially exploitable crash. This vulnerability affects Firefox ESR < 68.10, Firefox < 78, and Thunderbird < 68.10.0. **CVE ID : CVE-2020-12419**	N/A	A-MOZ-FIRE-100820/401
Use After Free	7/9/2020	9.3	When trying to connect to a STUN server, a race condition could have caused a use-after-free of a pointer, leading to memory corruption and a potentially exploitable crash. This vulnerability affects Firefox ESR < 68.10, Firefox < 78, and Thunderbird < 68.10.0. **CVE ID : CVE-2020-12420**	N/A	A-MOZ-FIRE-100820/402
Improper Certificate Validation	7/9/2020	4.3	When performing add-on updates, certificate chains terminating in non-built-in-roots were rejected (even if they were legitimately added by an administrator.) This could have caused add-ons to become out-of-date silently without notification to the user. This vulnerability affects Firefox ESR < 68.10,	N/A	A-MOZ-FIRE-100820/403

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Firefox < 78, and Thunderbird < 68.10.0. **CVE ID : CVE-2020-12421**		
thunderbird					
Missing Encryption of Sensitive Data	7/9/2020	4.3	If Thunderbird is configured to use STARTTLS for an IMAP server, and the server sends a PREAUTH response, then Thunderbird will continue with an unencrypted connection, causing email data to be sent without protection. This vulnerability affects Thunderbird < 68.9.0. **CVE ID : CVE-2020-12398**	N/A	A-MOZ-THUN-100820/404
Information Exposure Through Discrepancy	7/9/2020	1.2	NSS has shown timing differences when performing DSA signatures, which was exploitable and could eventually leak private keys. This vulnerability affects Thunderbird < 68.9.0, Firefox < 77, and Firefox ESR < 68.9. **CVE ID : CVE-2020-12399**	N/A	A-MOZ-THUN-100820/405
Use After Free	7/9/2020	2.6	When browsing a malicious page, a race condition in our SharedWorkerService could occur and lead to a potentially exploitable crash. This vulnerability affects Thunderbird < 68.9.0, Firefox < 77, and Firefox ESR < 68.9.	N/A	A-MOZ-THUN-100820/406

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		🟩	**CVE ID : CVE-2020-12405**		
Insufficient Verification of Data Authenticity	7/9/2020	9.3	Mozilla Developer Iain Ireland discovered a missing type check during unboxed objects removal, resulting in a crash. We presume that with enough effort that it could be exploited to run arbitrary code. This vulnerability affects Thunderbird < 68.9.0, Firefox < 77, and Firefox ESR < 68.9. **CVE ID : CVE-2020-12406**	N/A	A-MOZ-THUN-100820/407
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/9/2020	9.3	Due to confusion about ValueTags on JavaScript Objects, an object may pass through the type barrier, resulting in memory corruption and a potentially exploitable crash. *Note: this issue only affects Firefox on ARM64 platforms.* This vulnerability affects Firefox ESR < 68.10, Firefox < 78, and Thunderbird < 68.10.0. **CVE ID : CVE-2020-12417**	N/A	A-MOZ-THUN-100820/408
Out-of-bounds Read	7/9/2020	4.3	Manipulating individual parts of a URL object could have caused an out-of-bounds read, leaking process memory to malicious JavaScript. This vulnerability affects Firefox ESR < 68.10, Firefox < 78, and Thunderbird < 68.10.0.	N/A	A-MOZ-THUN-100820/409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-12418		
Use After Free	7/9/2020	9.3	When processing callbacks that occurred during window flushing in the parent process, the associated window may die; causing a use-after-free condition. This could have led to memory corruption and a potentially exploitable crash. This vulnerability affects Firefox ESR < 68.10, Firefox < 78, and Thunderbird < 68.10.0. **CVE ID : CVE-2020-12419**	N/A	A-MOZ-THUN-100820/410
Use After Free	7/9/2020	9.3	When trying to connect to a STUN server, a race condition could have caused a use-after-free of a pointer, leading to memory corruption and a potentially exploitable crash. This vulnerability affects Firefox ESR < 68.10, Firefox < 78, and Thunderbird < 68.10.0. **CVE ID : CVE-2020-12420**	N/A	A-MOZ-THUN-100820/411
Improper Certificate Validation	7/9/2020	4.3	When performing add-on updates, certificate chains terminating in non-built-in-roots were rejected (even if they were legitimately added by an administrator.) This could have caused add-ons to become out-of-date silently without notification to the user. This vulnerability affects	N/A	A-MOZ-THUN-100820/412

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Firefox ESR < 68.10, Firefox < 78, and Thunderbird < 68.10.0. **CVE ID : CVE-2020-12421**		
mversion_project					
mversion					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	7/1/2020	4.6	The issue occurs because tagName user input is formatted inside the exec function is executed without any checks. **CVE ID : CVE-2020-7688**	N/A	A-MVE-MVER-100820/413
mxplayer					
mx_player					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	7/8/2020	5.8	MX Player Android App versions prior to v1.24.5, are vulnerable to a directory traversal vulnerability when user is using the MX Transfer feature in "Receive" mode. An attacker can exploit this by connecting to the MX Transfer session as a "sender" and sending a MessageType of "FILE_LIST" with a "name" field containing directory traversal characters (../). This will result in the file being transferred to the victim's phone, but being saved outside of the intended "/sdcard/MXshare" directory. In some instances, an attacker can	N/A	A-MXP-MX_P-100820/414

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			achieve remote code execution by writing ".odex" and ".vdex" files in the "oat" directory of the MX Player application. **CVE ID : CVE-2020-5764**		
nedi					
nedi					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/7/2020	3.5	NeDi 1.9C is vulnerable to a cross-site scripting (XSS) attack. The application allows an attacker to execute arbitrary JavaScript code via the Topology-Map.php xo parameter. **CVE ID : CVE-2020-15028**	N/A	A-NED-NEDI-100820/415
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/7/2020	3.5	NeDi 1.9C is vulnerable to cross-site scripting (XSS) attack. The application allows an attacker to execute arbitrary JavaScript code via the Assets-Management.php sn parameter. **CVE ID : CVE-2020-15029**	N/A	A-NED-NEDI-100820/416
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/7/2020	3.5	NeDi 1.9C is vulnerable to cross-site scripting (XSS) attack. The application allows an attacker to execute arbitrary JavaScript code via the Topology-Routes.php rtr parameter. **CVE ID : CVE-2020-15030**	N/A	A-NED-NEDI-100820/417
Improper Neutralization of Input During	7/7/2020	3.5	NeDi 1.9C is vulnerable to cross-site scripting (XSS) attack. The application	N/A	A-NED-NEDI-100820/418

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			allows an attacker to execute arbitrary JavaScript code via the Assets-Management.php chg parameter. **CVE ID : CVE-2020-15031**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/7/2020	3.5	NeDi 1.9C is vulnerable to cross-site scripting (XSS) attack. The application allows an attacker to execute arbitrary JavaScript code via the Monitoring-Incidents.php id parameter. **CVE ID : CVE-2020-15032**	N/A	A-NED-NEDI-100820/419
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/7/2020	3.5	NeDi 1.9C is vulnerable to cross-site scripting (XSS) attack. The application allows an attacker to execute arbitrary JavaScript code via the snmpget.php ip parameter. **CVE ID : CVE-2020-15033**	N/A	A-NED-NEDI-100820/420
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/7/2020	3.5	NeDi 1.9C is vulnerable to cross-site scripting (XSS) attack. The application allows an attacker to execute arbitrary JavaScript code via the Monitoring-Setup.php tet parameter. **CVE ID : CVE-2020-15034**	N/A	A-NED-NEDI-100820/421
Improper Neutralization of Input During Web Page Generation ('Cross-site	7/7/2020	3.5	NeDi 1.9C is vulnerable to cross-site scripting (XSS) attack. The application allows an attacker to execute arbitrary JavaScript code via the Monitoring-Map.php hde	N/A	A-NED-NEDI-100820/422

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			parameter. **CVE ID : CVE-2020-15035**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/7/2020	3.5	NeDi 1.9C is vulnerable to cross-site scripting (XSS) attack. The application allows an attacker to execute arbitrary JavaScript code via the Topology-Linked.php dv parameter. **CVE ID : CVE-2020-15036**	N/A	A-NED-NEDI-100820/423
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/7/2020	3.5	NeDi 1.9C is vulnerable to cross-site scripting (XSS) attack. The application allows an attacker to execute arbitrary JavaScript code via the Reports-Devices.php page st[] parameter. **CVE ID : CVE-2020-15037**	N/A	A-NED-NEDI-100820/424
Netapp					
oncommand_insight					
N/A	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable	https://security.netapp.com/advisory/ntap-20200717-0004/	A-NET-ONCO-100820/425

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14632**		
snapcenter					
Information Exposure	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Roles). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2020-14641**	https://security.netapp.com/advisory/ntap-20200717-0004/	A-NET-SNAP-100820/426
N/A	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.48 and prior, 5.7.30 and prior and 8.0.20 and prior. Easily	https://security.netapp.com/advisory/ntap-20200717-0004/	A-NET-SNAP-100820/427

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14539**		
N/A	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 5.7.30 and prior and 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	https://security.netapp.com/advisory/ntap-20200717-0004/	A-NET-SNAP-100820/428

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14540		
Information Exposure	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2020-14634**	https://security.netapp.com/advisory/ntap-20200717-0004/	A-NET-SNAP-100820/429
oncommand_workflow_automation					
N/A	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or	https://security.netapp.com/advisory/ntap-20200717-0004/	A-NET-ONCO-100820/430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14632**		
oncommand_cloud_manager					
N/A	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14632**	https://security.netapp.com/advisory/ntap-20200717-0004/	A-NET-ONCO-100820/431
storagegrid_webscale_nas_bridge					
N/A	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that	https://security.netapp.com/advisory/ntap-20200717-	A-NET-STOR-100820/432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14632**	0004/	
e-series_santricity_os_controller					
N/A	7/15/2020	5.8	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/433

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2020-14556**		
N/A	7/15/2020	5	Vulnerability in the Java SE product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Java SE: 11.0.7 and 14.0.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/434

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ability to cause a partial denial of service (partial DOS) of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2020-14562**		
N/A	7/15/2020	4.3	Vulnerability in the Java SE product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Java SE: 11.0.7 and 14.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/435

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2020-14573**		
N/A	7/15/2020	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u261, 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2020-14577**		
N/A	7/15/2020	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u261 and 8u251; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/437

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2020-14578**		
N/A	7/15/2020	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u261 and 8u251; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/438

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2020-14579**		
N/A	7/15/2020	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/439

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			read access to a subset of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2020-14581**		
N/A	7/15/2020	5.1	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u261, 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/440

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2020-14583**		
N/A	7/15/2020	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 7u261, 8u251, 11.0.7 and 14.0.1; Java SE Embedded:	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/441

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			8u251. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 7.4 (Integrity impacts). CVSS Vector:		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:H/A:N). **CVE ID : CVE-2020-14593**		
e-series_santricity_storage_manager					
N/A	7/15/2020	5.8	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/442

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2020-14556**		
N/A	7/15/2020	5	Vulnerability in the Java SE product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Java SE: 11.0.7 and 14.0.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/443

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2020-14562**		
N/A	7/15/2020	4.3	Vulnerability in the Java SE product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Java SE: 11.0.7 and 14.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service.	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/444

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2020-14573**		
N/A	7/15/2020	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u261, 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service.	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/445

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2020-14577**		
N/A	7/15/2020	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u261 and 8u251; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/446

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			through a web service. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2020-14578**		
N/A	7/15/2020	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u261 and 8u251; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/447

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2020-14579**		
N/A	7/15/2020	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/448

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2020-14581**		
N/A	7/15/2020	5.1	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u261, 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/449

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2020-14583**		
N/A	7/15/2020	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 7u261, 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 7.4 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:H/A:N). **CVE ID : CVE-2020-14593**		
e-series_santricity_unified_manager					
N/A	7/15/2020	5.8	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/451

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2020-14556**		
N/A	7/15/2020	5	Vulnerability in the Java SE product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Java SE:	https://security.netapp.com/advisory/ntap-20200717-	A-NET-E-SE-100820/452

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			11.0.7 and 14.0.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2020-14562**	0005/	
N/A	7/15/2020	4.3	Vulnerability in the Java SE product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Java SE: 11.0.7 and 14.0.1. Difficult to exploit vulnerability	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/453

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2020-14573**		
N/A	7/15/2020	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u261, 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/454

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker with network access via TLS to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2020-14577**		
N/A	7/15/2020	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u261 and 8u251; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/455

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2020-14578**		
N/A	7/15/2020	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u261 and 8u251; Java SE Embedded: 8u251. Difficult to exploit	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2020-14579**		
N/A	7/15/2020	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251.	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/457

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2020-14581**		
N/A	7/15/2020	5.1	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u261, 8u251, 11.0.7 and 14.0.1; Java SE Embedded:	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14583		
N/A	7/15/2020	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 7u261, 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security.	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/459

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 7.4 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:H/A:N). **CVE ID : CVE-2020-14593**		
e-series_santricity_web_services_proxy					
N/A	7/15/2020	5.8	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/460

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2020-14556**		
N/A	7/15/2020	5	Vulnerability in the Java SE product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Java SE: 11.0.7 and 14.0.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/461

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2020-14562**		
N/A	7/15/2020	4.3	Vulnerability in the Java SE product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Java SE: 11.0.7 and 14.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/462

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2020-14573**		
N/A	7/15/2020	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u261, 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/463

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2020-14577**		
N/A	7/15/2020	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u261 and 8u251; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/464

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2020-14578**		
N/A	7/15/2020	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u261 and 8u251; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/465

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2020-14579**		
N/A	7/15/2020	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/466

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2020-14581**		
N/A	7/15/2020	5.1	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u261, 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2020-14583**		
N/A	7/15/2020	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 7u261, 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful	https://security.netapp.com/advisory/ntap-20200717-0005/	A-NET-E-SE-100820/468

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 7.4 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:H/A:N). **CVE ID : CVE-2020-14593**		
active_iq_unified_manager					
N/A	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle	https://security.netapp	A-NET-ACTI-100820/469

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MySQL (component: Server: Options). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14632**	.com/advisory/ntap-20200717-0004/	
Netflix					
titus					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	7/14/2020	7.5	Netflix Titus, all versions prior to version v0.1.1-rc.274, uses Java Bean Validation (JSR 380) custom constraint validators. When building custom constraint violation error messages, different types of interpolation are supported, including Java EL expressions. If an attacker can inject arbitrary data in the error message template being passed to	N/A	A-NET-TITU-100820/470

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ConstraintValidatorContext.buildConstraintViolationWithTemplate() argument, they will be able to run arbitrary Java code. **CVE ID : CVE-2020-9297**		
nexaweb					
nexacro_14					
Improper Input Validation	7/2/2020	7.5	Nexacro14/17 ExtCommonApiV13 Library under 2019.9.6 version contain a vulnerability that could allow remote attacker to execute arbitrary code by setting the arguments to the vulnerable API. This can be leveraged for code execution by rebooting the victim's PC **CVE ID : CVE-2020-7820**	http://support.tobesoft.co.kr/Support/index.html, https://www.krcert.or.kr/krcert/secNoticeView.do?bulletin_writing_sequence=35491	A-NEX-NEXA-100820/471
Improper Input Validation	7/2/2020	7.5	Nexacro14/17 ExtCommonApiV13 Library under 2019.9.6 version contain a vulnerability that could allow remote attacker to execute arbitrary code by modifying the value of registry path. This can be leveraged for code execution by rebooting the victim's PC **CVE ID : CVE-2020-7821**	http://support.tobesoft.co.kr/Support/index.html, https://www.krcert.or.kr/krcert/secNoticeView.do?bulletin_writing_sequence=35491	A-NEX-NEXA-100820/472
nexacro_17					
Improper Input Validation	7/2/2020	7.5	Nexacro14/17 ExtCommonApiV13 Library under 2019.9.6	http://support.tobesoft.co.kr/Supp	A-NEX-NEXA-100820/473

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			version contain a vulnerability that could allow remote attacker to execute arbitrary code by setting the arguments to the vulnerable API. This can be leveraged for code execution by rebooting the victim's PC **CVE ID : CVE-2020-7820**	ort/index.html, https://www.krcert.or.kr/krcert/secNoticeView.do?bulletin_writing_sequence=35491	
Improper Input Validation	7/2/2020	7.5	Nexacro14/17 ExtCommonApiV13 Library under 2019.9.6 version contain a vulnerability that could allow remote attacker to execute arbitrary code by modifying the value of registry path. This can be leveraged for code execution by rebooting the victim's PC **CVE ID : CVE-2020-7821**	http://support.tobesoft.co.kr/Support/index.html, https://www.krcert.or.kr/krcert/secNoticeView.do?bulletin_writing_sequence=35491	A-NEX-NEXA-100820/474
Nextcloud					
deck					
Improper Privilege Management	7/2/2020	4	Improper access control in Nextcloud Deck 1.0.0 allowed an attacker to inject tasks into other users decks. **CVE ID : CVE-2020-8179**	N/A	A-NEX-DECK-100820/475
contacts					
Unrestricted Upload of File with Dangerous Type	7/10/2020	4	A missing file type check in Nextcloud Contacts 3.2.0 allowed a malicious user to upload any file as avatars. **CVE ID : CVE-2020-8181**	N/A	A-NEX-CONT-100820/476

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
node.bcrypt.js_project					
node.bcrypt.js					
Inadequate Encryption Strength	7/1/2020	4.3	Data is truncated wrong when its length is greater than 255 bytes. **CVE ID : CVE-2020-7689**	N/A	A-NOD-NODE-100820/477
nordicsemi					
android_ble_library					
Missing Encryption of Sensitive Data	7/7/2020	3.3	Nordic Semiconductor Android BLE Library through 2.2.1 and DFU Library through 1.10.4 for Android (as used by nRF Connect and other applications) can engage in unencrypted communication while showing the user that the communication is purportedly encrypted. The problem is in bond creation (e.g., internalCreateBond in BleManagerHandler). **CVE ID : CVE-2020-15509**	N/A	A-NOR-ANDR-100820/478
dfu_library					
Missing Encryption of Sensitive Data	7/7/2020	3.3	Nordic Semiconductor Android BLE Library through 2.2.1 and DFU Library through 1.10.4 for Android (as used by nRF Connect and other applications) can engage in unencrypted communication while showing the user that the communication is purportedly encrypted.	N/A	A-NOR-DFU_-100820/479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			The problem is in bond creation (e.g., internalCreateBond in BleManagerHandler). **CVE ID : CVE-2020-15509**		
northwestern					
timelinejs					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/9/2020	3.5	In TimelineJS before version 3.7.0, some user data renders as HTML. An attacker could implement an XSS exploit with maliciously crafted content in a number of data fields. This risk is present whether the source data for the timeline is stored on Google Sheets or in a JSON configuration file. Most TimelineJS users configure their timeline with a Google Sheets document. Those users are exposed to this vulnerability if they grant write access to the document to a malicious inside attacker, if the access of a trusted user is compromised, or if they grant public write access to the document. Some TimelineJS users configure their timeline with a JSON document. Those users are exposed to this vulnerability if they grant write access to the document to a malicious inside attacker, if the	https://github.com/NUKnightLab/TimelineJS3/security/advisories/GHSA-2jpm-827p-j44g	A-NOR-TIME-100820/480

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access of a trusted user is compromised, or if write access to the system hosting that document is otherwise compromised. Version 3.7.0 of TimelineJS addresses this in two ways. For content which is intended to support limited HTML markup for styling and linking, that content is "sanitized" before being added to the DOM. For content intended for simple text display, all markup is stripped. Very few users of TimelineJS actually install the TimelineJS code on their server. Most users publish a timeline using a URL hosted on systems we control. The fix for this issue is published to our system such that **those users will automatically begin using the new code**. The only exception would be users who have deliberately edited the embed URL to "pin" their timeline to an earlier version of the code. Some users of TimelineJS use it as a part of a wordpress plugin (knight-lab-timelinejs). Version 3.7.0.0 of that plugin and newer integrate the updated code. Users are encouraged to update the		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			plugin rather than manually update the embedded version of TimelineJS. **CVE ID : CVE-2020-15092**		
Ntop					
ndpi					
Out-of-bounds Read	7/1/2020	6.4	In nDPI through 3.2, the packet parsing code is vulnerable to a heap-based buffer over-read in ndpi_parse_packet_line_info in lib/ndpi_main.c. **CVE ID : CVE-2020-15471**	N/A	A-NTO-NDPI-100820/481
Out-of-bounds Read	7/1/2020	6.4	In nDPI through 3.2, the H.323 dissector is vulnerable to a heap-based buffer over-read in ndpi_search_h323 in lib/protocols/h323.c, as demonstrated by a payload packet length that is too short. **CVE ID : CVE-2020-15472**	N/A	A-NTO-NDPI-100820/482
Out-of-bounds Read	7/1/2020	6.4	In nDPI through 3.2, the OpenVPN dissector is vulnerable to a heap-based buffer over-read in ndpi_search_openvpn in lib/protocols/openvpn.c. **CVE ID : CVE-2020-15473**	N/A	A-NTO-NDPI-100820/483
Out-of-bounds Write	7/1/2020	7.5	In nDPI through 3.2, there is a stack overflow in extractRDNSequence in lib/protocols/tls.c. **CVE ID : CVE-2020-15474**	N/A	A-NTO-NDPI-100820/484
Use After Free	7/1/2020	7.5	In nDPI through 3.2,	N/A	A-NTO-NDPI-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ndpi_reset_packet_line_info in lib/ndpi_main.c omits certain reinitialization, leading to a use-after-free. **CVE ID : CVE-2020-15475**		100820/485
Out-of-bounds Read	7/1/2020	5	In nDPI through 3.2, the Oracle protocol dissector has a heap-based buffer over-read in ndpi_search_oracle in lib/protocols/oracle.c. **CVE ID : CVE-2020-15476**	N/A	A-NTO-NDPI-100820/486
Nvidia					
jetpack_software_development_kit					
Incorrect Default Permissions	7/8/2020	4.6	NVIDIA JetPack SDK, version 4.2 and 4.3, contains a vulnerability in its installation scripts in which permissions are incorrectly set on certain directories, which can lead to escalation of privileges. **CVE ID : CVE-2020-5974**	https://nvidia.custhelp.com/app/answers/detail/a_id/5039	A-NVI-JETP-100820/487
Octobercms					
october					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/14/2020	3.5	In October from version 1.0.319 and before version 1.0.466, a user with access to a markdown FormWidget that stores data persistently could create a stored XSS attack against themselves and any other users with access to the generated HTML from the field. This has been fixed in 1.0.466. For users of the	https://github.com/octobercms/october/security/advisories/GHSA-w4pj-7p68-3vgv	A-OCT-OCTO-100820/488

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			RainLab.Blog plugin, this has also been fixed in 1.4.1. **CVE ID : CVE-2020-11083**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/2/2020	3.5	In October from version 1.0.319 and before version 1.0.467, pasting content copied from malicious websites into the Froala richeditor could result in a successful self-XSS attack. This has been fixed in 1.0.467. **CVE ID : CVE-2020-4061**	https://github.com/octobercms/october/security/advisories/GHSA-3pc2-fm7p-q2vg	A-OCT-OCTO-100820/489
online_hotel_booking_system_project					
online_hotel_booking_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/5/2020	4.3	An issue was discovered in the bestsoftinc Hotel Booking System Pro plugin through 1.1 for WordPress. Persistent XSS can occur via any of the registration fields. **CVE ID : CVE-2020-15536**	N/A	A-ONL-ONLI-100820/490
openenclave					
openenclave					
N/A	7/15/2020	1.2	In openenclave before 0.10.0, enclaves that use x87 FPU operations are vulnerable to tampering by a malicious host application. By violating the Linux System V Application Binary Interface (ABI) for such operations, a host app can compromise the execution integrity of some x87 FPU operations in an enclave.	https://github.com/openenclave/openenclave/security/advisories/GHSA-7wjx-wcwg-w999	A-OPE-OPEN-100820/491

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Depending on the FPU control configuration of the enclave app and whether the operations are used in secret-dependent execution paths, this vulnerability may also be used to mount a side-channel attack on the enclave. This has been fixed in 0.10.0 and the current master branch. Users will need to recompile their applications against the patched libraries to be protected from this vulnerability. **CVE ID : CVE-2020-15107**		
Openldap					
openldap					
Improper Certificate Validation	7/14/2020	4	libldap in certain third-party OpenLDAP packages has a certificate-validation flaw when the third-party package is asserting RFC6125 support. It considers CN even when there is a non-matching subjectAltName (SAN). This is fixed in, for example, openldap-2.4.46-10.el8 in Red Hat Enterprise Linux. **CVE ID : CVE-2020-15719**	N/A	A-OPE-OPEN-100820/492
Opensis					
opensis					
Improper Neutralization	7/1/2020	7.5	openSIS before 7.4 allows	https://github.com/OS	A-OPE-OPEN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Special Elements used in an SQL Command ('SQL Injection')			SQL Injection. **CVE ID : CVE-2020-13380**	4ED/openSIS-Responsive-Design/commit/1127ae0bb7c3a2883febeabc6b71ad8d73510de8	100820/493
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	7/1/2020	7.5	openSIS through 7.4 allows SQL Injection. **CVE ID : CVE-2020-13381**	N/A	A-OPE-OPEN-100820/494
Improper Privilege Management	7/1/2020	6.4	openSIS through 7.4 has Incorrect Access Control. **CVE ID : CVE-2020-13382**	N/A	A-OPE-OPEN-100820/495
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	7/1/2020	5	openSIS through 7.4 allows Directory Traversal. **CVE ID : CVE-2020-13383**	N/A	A-OPE-OPEN-100820/496
openthread					
wpantund					
Improper Release of Memory Before Removing Last Reference	7/7/2020	2.1	A memory leak in Openthread's wpantund versions up to commit 0e5d1601febb869f583e944785e5685c6c747be7, when used in an environment where wpanctl is directly interfacing with the control driver (eg: debug	https://github.com/openthread/wpantund/pull/468/commits/0e5d1601febb869f583e944785e5685c6c747be7	A-OPE-WPAN-100820/497

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			environments) can allow an attacker to crash the service (DoS). We recommend updating, or to restrict access in your debug environments. **CVE ID : CVE-2020-8916**		
Openvpn					
openvpn_access_server					
Insufficient Session Expiration	7/14/2020	5	OpenVPN Access Server older than version 2.8.4 generates new user authentication tokens instead of reusing exiting tokens on reconnect making it possible to circumvent the initial token expiry timestamp. **CVE ID : CVE-2020-15074**	https://openvpn.net/vpn-server-resources/release-notes/	A-OPE-OPEN-100820/498
Oracle					
application_express					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/15/2020	3.5	Vulnerability in the Oracle Application Express component of Oracle Database Server. Supported versions that are affected are 5.1-19.2. Easily exploitable vulnerability allows low privileged attacker having SQL Workshop privilege with network access via HTTP to compromise Oracle Application Express. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle	N/A	A-ORA-APPL-100820/499

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Application Express, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Express accessible data as well as unauthorized read access to a subset of Oracle Application Express accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2020-2513**		
N/A	7/15/2020	4.9	Vulnerability in the Oracle Application Express component of Oracle Database Server. Supported versions that are affected are 5.1-19.2. Easily exploitable vulnerability allows low privileged attacker having SQL Workshop privilege with network access via HTTP to compromise Oracle Application Express. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Express, attacks may significantly	N/A	A-ORA-APPL-100820/500

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Express accessible data as well as unauthorized read access to a subset of Oracle Application Express accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2020-2971**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/15/2020	3.5	Vulnerability in the Oracle Application Express component of Oracle Database Server. Supported versions that are affected are 5.1-19.2. Easily exploitable vulnerability allows low privileged attacker having SQL Workshop privilege with network access via HTTP to compromise Oracle Application Express. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Express, attacks may significantly impact additional products. Successful	N/A	A-ORA-APPL-100820/501

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Express accessible data as well as unauthorized read access to a subset of Oracle Application Express accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2020-2972**		
N/A	7/15/2020	3.5	Vulnerability in the Oracle Application Express component of Oracle Database Server. Supported versions that are affected are 5.1-19.2. Easily exploitable vulnerability allows low privileged attacker having SQL Workshop privilege with network access via HTTP to compromise Oracle Application Express. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Express, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized	N/A	A-ORA-APPL-100820/502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			update, insert or delete access to some of Oracle Application Express accessible data as well as unauthorized read access to a subset of Oracle Application Express accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2020-2973**		
N/A	7/15/2020	3.5	Vulnerability in the Oracle Application Express component of Oracle Database Server. Supported versions that are affected are 5.1-19.2. Easily exploitable vulnerability allows low privileged attacker having SQL Workshop privilege with network access via HTTP to compromise Oracle Application Express. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Express, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle	N/A	A-ORA-APPL-100820/503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Application Express accessible data as well as unauthorized read access to a subset of Oracle Application Express accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2020-2974**		
N/A	7/15/2020	3.5	Vulnerability in the Oracle Application Express component of Oracle Database Server. Supported versions that are affected are 5.1-19.2. Easily exploitable vulnerability allows low privileged attacker having SQL Workshop privilege with network access via HTTP to compromise Oracle Application Express. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Express, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Express accessible data as well as	N/A	A-ORA-APPL-100820/504

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized read access to a subset of Oracle Application Express accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2020-2975**		
N/A	7/15/2020	3.5	Vulnerability in the Oracle Application Express component of Oracle Database Server. Supported versions that are affected are 5.1-19.2. Easily exploitable vulnerability allows low privileged attacker having SQL Workshop privilege with network access via HTTP to compromise Oracle Application Express. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Express, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Express accessible data as well as unauthorized read access to a subset of Oracle	N/A	A-ORA-APPL-100820/505

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Application Express accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2020-2976**		
N/A	7/15/2020	4.9	Vulnerability in the Oracle Application Express component of Oracle Database Server. Supported versions that are affected are 5.1-19.2. Easily exploitable vulnerability allows low privileged attacker having Valid User Account privilege with network access via HTTP to compromise Oracle Application Express. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Express accessible data as well as unauthorized read access to a subset of Oracle Application Express accessible data. CVSS 3.1 Base Score 4.6 (Confidentiality and Integrity impacts). CVSS Vector:	N/A	A-ORA-APPL-100820/506

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N). **CVE ID : CVE-2020-2977**		
e-business_intelligence					
N/A	7/15/2020	5.8	Vulnerability in the Oracle E-Business Intelligence product of Oracle E-Business Suite (component: DBI Setups). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle E-Business Intelligence. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle E-Business Intelligence, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle E-Business Intelligence accessible data as well as unauthorized update, insert or delete access to some of Oracle E-Business Intelligence accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS	N/A	A-ORA-E-BU-100820/507

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2020-14668**		
N/A	7/15/2020	5.8	Vulnerability in the Oracle E-Business Intelligence product of Oracle E-Business Suite (component: DBI Setups). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle E-Business Intelligence. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle E-Business Intelligence, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle E-Business Intelligence accessible data as well as unauthorized update, insert or delete access to some of Oracle E-Business Intelligence accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector:	N/A	A-ORA-E-BU-100820/508

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2020-14681**		
customer_relationship_management_gateway_for_mobile_devices					
N/A	7/15/2020	6.4	Vulnerability in the Oracle CRM Gateway for Mobile Devices product of Oracle E-Business Suite (component: Setup of Mobile Applications). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Gateway for Mobile Devices. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle CRM Gateway for Mobile Devices accessible data as well as unauthorized access to critical data or complete access to all Oracle CRM Gateway for Mobile Devices accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2020-14598**	N/A	A-ORA-CUST-100820/509
N/A	7/15/2020	6.4	Vulnerability in the Oracle CRM Gateway for Mobile	N/A	A-ORA-CUST-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Devices product of Oracle E-Business Suite (component: Setup of Mobile Applications). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Gateway for Mobile Devices. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle CRM Gateway for Mobile Devices accessible data as well as unauthorized access to critical data or complete access to all Oracle CRM Gateway for Mobile Devices accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2020-14599**		100820/510
depot_repair					
N/A	7/15/2020	5.8	Vulnerability in the Oracle Depot Repair product of Oracle E-Business Suite (component: Estimate and Actual Charges). Supported versions that are affected are 12.1.1-12.1.3. Easily	N/A	A-ORA-DEPO-100820/511

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Depot Repair. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Depot Repair, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Depot Repair accessible data as well as unauthorized update, insert or delete access to some of Oracle Depot Repair accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2020-14682**		
financial_services_liquidity_risk_management					
N/A	7/15/2020	5.5	Vulnerability in the Oracle Financial Services Liquidity Risk Management product of Oracle Financial Services Applications (component: User Interface). The supported version that is affected is 8.0.6. Easily	N/A	A-ORA-FINA-100820/512

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Liquidity Risk Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financial Services Liquidity Risk Management accessible data as well as unauthorized read access to a subset of Oracle Financial Services Liquidity Risk Management accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N). **CVE ID : CVE-2020-14691**		
coherence					
Improper Resource Shutdown or Release	7/15/2020	7.8	Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: CacheStore). Supported versions that are affected are 3.7.1.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows	N/A	A-ORA-COHE-100820/513

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker with network access via HTTP to compromise Oracle Coherence. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Coherence. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR: N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14642**		
insurance_accounting_analyzer					
N/A	7/15/2020	4	Vulnerability in the Oracle Insurance Accounting Analyzer product of Oracle Financial Services Applications (component: User Interface). Supported versions that are affected are 8.0.6-8.0.9. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Insurance Accounting Analyzer. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Insurance Accounting Analyzer accessible data. CVSS 3.1 Base Score 6.5	N/A	A-ORA-INSU-100820/514

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2020-14693**		
financial_services_loan_loss_forecasting_and_provisioning					
N/A	7/15/2020	4	Vulnerability in the Oracle Financial Services Loan Loss Forecasting and Provisioning product of Oracle Financial Services Applications (component: User Interface). Supported versions that are affected are 8.0.6-8.0.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Loan Loss Forecasting and Provisioning. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financial Services Loan Loss Forecasting and Provisioning accessible data. CVSS 3.1 Base Score 6.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2020-14692**	N/A	A-ORA-FINA-100820/515
retail_customer_management_and_segmentation_foundation					
N/A	7/15/2020	4	Vulnerability in the	N/A	A-ORA-RETA-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Customer Management and Segmentation Foundation product of Oracle Retail Applications (component: Segment). Supported versions that are affected are 16.0, 17.0 and 18.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Customer Management and Segmentation Foundation. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Customer Management and Segmentation Foundation accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2020-14708**		100820/516
N/A	7/15/2020	5.5	Vulnerability in the Customer Management and Segmentation Foundation product of Oracle Retail Applications (component: Card). Supported versions that are affected are 16.0, 17.0 and 18.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Customer Management and	N/A	A-ORA-RETA-100820/517

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Segmentation Foundation. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Customer Management and Segmentation Foundation accessible data as well as unauthorized read access to a subset of Customer Management and Segmentation Foundation accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N). **CVE ID : CVE-2020-14709**		
N/A	7/15/2020	5.5	Vulnerability in the Customer Management and Segmentation Foundation product of Oracle Retail Applications (component: Security). Supported versions that are affected are 16.0, 17.0 and 18.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Customer Management and Segmentation Foundation. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Customer	N/A	A-ORA-RETA-100820/518

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Management and Segmentation Foundation accessible data as well as unauthorized read access to a subset of Customer Management and Segmentation Foundation accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2020-14710**		
autovue					
N/A	7/15/2020	4	Vulnerability in the Oracle AutoVue product of Oracle Supply Chain (component: Security). The supported version that is affected is 21.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle AutoVue. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle AutoVue accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2020-14551**	N/A	A-ORA-AUTO-100820/519
enterprise_manager_base_platform					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	7/15/2020	5.5	Vulnerability in the Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Enterprise Config Management). Supported versions that are affected are 13.3.0.0 and 13.4.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Enterprise Manager Base Platform. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Enterprise Manager Base Platform accessible data as well as unauthorized update, insert or delete access to some of Enterprise Manager Base Platform accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N). **CVE ID : CVE-2020-2982**	N/A	A-ORA-ENTE-100820/520
ilearning					
N/A	7/15/2020	6.4	Vulnerability in the Oracle iLearning product of Oracle iLearning (component: Assessment Manager). Supported	N/A	A-ORA-ILEA-100820/521

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions that are affected are 6.1 and 6.1.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iLearning. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iLearning accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle iLearning. CVSS 3.1 Base Score 8.2 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:L). **CVE ID : CVE-2020-14595**		
mysql					
N/A	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.30 and prior and 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can	https://security.netapp.com/advisory/ntap-20200717-0004/	A-ORA-MYSQ-100820/522

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14547**		
N/A	7/15/2020	3.5	Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.6.48 and prior, 5.7.30 and prior and 8.0.20 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Client. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14550**	N/A	A-ORA-MYSQ-100820/523
N/A	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Pluggable Auth). Supported versions that	https://security.netapp.com/advisory/ntap-20200717-	A-ORA-MYSQ-100820/524

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			are affected are 5.7.30 and prior and 8.0.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2020-14553**	0004/	
N/A	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 5.6.48 and prior, 5.7.30 and prior and 8.0.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality	https://security.netapp.com/advisory/ntap-20200717-0004/	A-ORA-MYSQ-100820/525

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2020-14559**		
N/A	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.29 and prior and 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14567**	https://security.netapp.com/advisory/ntap-20200717-0004/	A-ORA-MYSQ-100820/526
N/A	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise	https://security.netapp.com/advisory/ntap-20200717-0004/	A-ORA-MYSQ-100820/527

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14568**		
Information Exposure	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Roles). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2020-14641**	https://security.netapp.com/advisory/ntap-20200717-0004/	A-ORA-MYSQ-100820/528
N/A	7/15/2020	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Roles).	https://security.netapp.com/advisory/ntap-	A-ORA-MYSQ-100820/529

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2020-14643**	20200717-0004/	
N/A	7/15/2020	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Roles). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or	https://security.netapp.com/advisory/ntap-20200717-0004/	A-ORA-MYSQ-100820/530

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2020-14651**		
N/A	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14654**	https://security.netapp.com/advisory/ntap-20200717-0004/	A-ORA-MYSQ-100820/531
N/A	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle MySQL (component:	https://security.netapp.com/advis	A-ORA-MYSQ-100820/532

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Server: Locking). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14656**	ory/ntap-20200717-0004/	
N/A	7/15/2020	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector:	https://security.netapp.com/advisory/ntap-20200717-0004/	A-ORA-MYSQ-100820/533

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2020-14697**		
N/A	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14702**	https://security.netapp.com/advisory/ntap-20200717-0004/	A-ORA-MYSQ-100820/534
N/A	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.48 and prior, 5.7.30 and prior and 8.0.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise	https://security.netapp.com/advisory/ntap-20200717-0004/	A-ORA-MYSQ-100820/535

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14539**		
N/A	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 5.7.30 and prior and 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14540**	https://security.netapp.com/advisory/ntap-20200717-0004/	A-ORA-MYSQ-100820/536
N/A	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported	https://security.netapp.com/advisory/ntap-	A-ORA-MYSQ-100820/537

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14575**	20200717-0004/	
N/A	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: UDF). Supported versions that are affected are 5.7.30 and prior and 8.0.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:	https://security.netapp.com/advisory/ntap-20200717-0004/	A-ORA-MYSQ-100820/538

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14576**		
N/A	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14586**	https://security.netapp.com/advisory/ntap-20200717-0004/	A-ORA-MYSQ-100820/539
N/A	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Audit Plug-in). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can	https://security.netapp.com/advisory/ntap-20200717-0004/	A-ORA-MYSQ-100820/540

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14591**		
N/A	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14597**	https://security.netapp.com/advisory/ntap-20200717-0004/	A-ORA-MYSQ-100820/541
N/A	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.20 and	https://security.netapp.com/advisory/ntap-20200717-0004/	A-ORA-MYSQ-100820/542

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14614**		
N/A	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	https://security.netapp.com/advisory/ntap-20200717-0004/	A-ORA-MYSQ-100820/543

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14619		
N/A	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14620**	https://security.netapp.com/advisory/ntap-20200717-0004/	A-ORA-MYSQ-100820/544
N/A	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable	https://security.netapp.com/advisory/ntap-20200717-0004/	A-ORA-MYSQ-100820/545

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14623**		
N/A	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: JSON). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14624**	https://security.netapp.com/advisory/ntap-20200717-0004/	A-ORA-MYSQ-100820/546
N/A	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Audit). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via	https://security.netapp.com/advisory/ntap-20200717-0004/	A-ORA-MYSQ-100820/547

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14631**		
N/A	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14632**	https://security.netapp.com/advisory/ntap-20200717-0004/	A-ORA-MYSQ-100820/548
N/A	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle	https://security.netapp	A-ORA-MYSQ-100820/549

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MySQL (component: InnoDB). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2020-14633**	.com/advisory/ntap-20200717-0004/	
Information Exposure	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:	https://security.netapp.com/advisory/ntap-20200717-0004/	A-ORA-MYSQ-100820/550

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			H/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2020-14634**		
N/A	7/15/2020	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2020-14663**	https://security.netapp.com/advisory/ntap-20200717-0004/	A-ORA-MYSQ-100820/551
N/A	7/15/2020	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in takeover of	https://security.netapp.com/advisory/ntap-20200717-0004/	A-ORA-MYSQ-100820/552

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MySQL Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2020-14678**		
N/A	7/15/2020	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14680**	https://security.netapp.com/advisory/ntap-20200717-0004/	A-ORA-MYSQ-100820/553
jdk					
N/A	7/15/2020	5.8	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 8u251, 11.0.7 and 14.0.1;	https://security.netapp.com/advisory/ntap-20200717-0005/	A-ORA-JDK-100820/554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2020-14556**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	7/15/2020	5	Vulnerability in the Java SE product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Java SE: 11.0.7 and 14.0.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2020-14562**	https://security.netapp.com/advisory/ntap-20200717-0005/	A-ORA-JDK-100820/555
N/A	7/15/2020	4.3	Vulnerability in the Java SE product of Oracle Java SE	https://security.netapp	A-ORA-JDK-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(component: Hotspot). Supported versions that are affected are Java SE: 11.0.7 and 14.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2020-14573**	.com/advisory/ntap-20200717-0005/	100820/556
N/A	7/15/2020	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JSSE). Supported versions that	https://security.netapp.com/advisory/ntap-20200717-	A-ORA-JDK-100820/557

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			are affected are Java SE: 7u261, 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2020-14577**	0005/	
N/A	7/15/2020	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that	https://security.netapp.com/advisory/ntap-20200717-	A-ORA-JDK-100820/558

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			are affected are Java SE: 7u261 and 8u251; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2020-14578**	0005/	
N/A	7/15/2020	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries).	https://security.netapp.com/advisory/ntap-	A-ORA-JDK-100820/559

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Supported versions that are affected are Java SE: 7u261 and 8u251; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2020-14579**	20200717-0005/	
N/A	7/15/2020	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE	https://security.netapp.com/advis	A-ORA-JDK-100820/560

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(component: 2D). Supported versions that are affected are Java SE: 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2020-14581**	ory/ntap-20200717-0005/	
N/A	7/15/2020	5.1	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE	https://security.netapp.com/advis	A-ORA-JDK-100820/561

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(component: Libraries). Supported versions that are affected are Java SE: 7u261, 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 8.3	ory/ntap-20200717-0005/	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2020-14583**		
N/A	7/15/2020	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 7u261, 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed	https://security.netapp.com/advisory/ntap-20200717-0005/	A-ORA-JDK-100820/562

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 7.4 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:H/A:N). **CVE ID : CVE-2020-14593**		
N/A	7/15/2020	5	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JAXP). Supported versions that are affected are Java SE: 7u261, 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data. Note: This vulnerability can only be exploited by supplying data to APIs in the	https://security.netapp.com/advisory/ntap-20200717-0005/	A-ORA-JDK-100820/563

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2020-14621**		
N/A	7/15/2020	5.1	Vulnerability in the Java SE product of Oracle Java SE (component: JavaFX). The supported version that is affected is Java SE: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g.,	https://security.netapp.com/advisory/ntap-20200717-0005/	A-ORA-JDK-100820/564

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2020-14664**		
jre					
N/A	7/15/2020	5.8	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java	https://security.netapp.com/advisory/ntap-20200717-0005/	A-ORA-JRE-100820/565

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2020-14556**		
N/A	7/15/2020	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u261, 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access	https://security.netapp.com/advisory/ntap-20200717-0005/	A-ORA-JRE-100820/566

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to a subset of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2020-14577**		
N/A	7/15/2020	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u261 and 8u251; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized	https://security.netapp.com/advisory/ntap-20200717-0005/	A-ORA-JRE-100820/567

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2020-14578**		
N/A	7/15/2020	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u261 and 8u251; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability	https://security.netapp.com/advisory/ntap-20200717-0005/	A-ORA-JRE-100820/568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2020-14579**		
N/A	7/15/2020	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful	https://security.netapp.com/advisory/ntap-20200717-0005/	A-ORA-JRE-100820/569

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2020-14581**		
N/A	7/15/2020	5.1	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u261, 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful	https://security.netapp.com/advisory/ntap-20200717-0005/	A-ORA-JRE-100820/570

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2020-14583**		
N/A	7/15/2020	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE:	https://security.netapp.com/advisory/ntap-20200717-	A-ORA-JRE-100820/571

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			7u261, 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 7.4	0005/	

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:H/A:N). **CVE ID : CVE-2020-14593**		
N/A	7/15/2020	5	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JAXP). Supported versions that are affected are Java SE: 7u261, 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).	https://security.netapp.com/advisory/ntap-20200717-0005/	A-ORA-JRE-100820/572

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14621		
N/A	7/15/2020	5.1	Vulnerability in the Java SE product of Oracle Java SE (component: JavaFX). The supported version that is affected is Java SE: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity	https://security.netapp.com/advisory/ntap-20200717-0005/	A-ORA-JRE-100820/573

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2020-14664**		
webcenter_portal					
N/A	7/15/2020	3.5	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Security Framework). Supported versions that are affected are 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Portal. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Portal, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebCenter Portal accessible data. CVSS 3.1 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:N/A:N).	N/A	A-ORA-WEBC-100820/574

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14552		
N/A	7/15/2020	7.5	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Composer). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Portal. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Portal accessible data as well as unauthorized read access to a subset of Oracle WebCenter Portal accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebCenter Portal. CVSS 3.1 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L). **CVE ID : CVE-2020-14611**	N/A	A-ORA-WEBC-100820/575
vm_virtualbox					
N/A	7/15/2020	4.4	Vulnerability in the Oracle VM VirtualBox product of	N/A	A-ORA-VM_V-100820/576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 and prior to 6.1.12. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2020-14646**		
N/A	7/15/2020	4.4	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 and prior to 6.1.12. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox	N/A	A-ORA-VM_V-100820/577

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2020-14647**		
N/A	7/15/2020	4.7	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 and prior to 6.1.12. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all	N/A	A-ORA-VM_V-100820/578

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N). **CVE ID : CVE-2020-14648**		
N/A	7/15/2020	4.4	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 and prior to 6.1.12. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2020-14649**	N/A	A-ORA-VM_V-100820/579
N/A	7/15/2020	4.7	Vulnerability in the Oracle VM VirtualBox product of	N/A	A-ORA-VM_V-100820/580

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 and prior to 6.1.12. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N). **CVE ID : CVE-2020-14650**		
Out-of-bounds Read	7/15/2020	4.7	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 and prior to 6.1.12. Difficult to exploit vulnerability allows high privileged attacker with logon to the	N/A	A-ORA-VM_V-100820/581

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N). **CVE ID : CVE-2020-14694**		
Out-of-bounds Read	7/15/2020	4.7	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 and prior to 6.1.12. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful	N/A	A-ORA-VM_V-100820/582

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N). **CVE ID : CVE-2020-14695**		
Out-of-bounds Read	7/15/2020	4.7	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 and prior to 6.1.12. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector:	N/A	A-ORA-VM_V-100820/583

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N). **CVE ID : CVE-2020-14698**		
Integer Underflow (Wrap or Wraparound)	7/15/2020	4.4	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 and prior to 6.1.12. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2020-14699**	N/A	A-ORA-VM_V-100820/584
Out-of-bounds Read	7/15/2020	4.7	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 and	N/A	A-ORA-VM_V-100820/585

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 6.1.12. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N). **CVE ID : CVE-2020-14700**		
Use of Uninitialized Resource	7/15/2020	4.9	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 and prior to 6.1.12. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is	N/A	A-ORA-VM_V-100820/586

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N). **CVE ID : CVE-2020-14703**		
Use of Uninitialized Resource	7/15/2020	4.9	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 and prior to 6.1.12. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox	N/A	A-ORA-VM_V-100820/587

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N). **CVE ID : CVE-2020-14704**		
N/A	7/15/2020	1.9	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 and prior to 6.1.12. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 5.0 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14707**	N/A	A-ORA-VM_V-100820/588
N/A	7/15/2020	4.4	Vulnerability in the Oracle VM VirtualBox product of	N/A	A-ORA-VM_V-100820/589

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 and prior to 6.1.12. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. Note: The CVE-2020-14711 is applicable to macOS host only. CVSS 3.1 Base Score 6.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2020-14711**		
N/A	7/15/2020	1.9	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 and prior to 6.1.12. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where	N/A	A-ORA-VM_V-100820/590

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 5.0 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:H/A:N). **CVE ID : CVE-2020-14712**		
N/A	7/15/2020	4.4	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 and prior to 6.1.12. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of	N/A	A-ORA-VM_V-100820/591

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2020-14713**		
N/A	7/15/2020	2.1	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 and prior to 6.1.12. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14714**	N/A	A-ORA-VM_V-100820/592
N/A	7/15/2020	2.1	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that	N/A	A-ORA-VM_V-100820/593

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			are affected are Prior to 5.2.44, prior to 6.0.24 and prior to 6.1.12. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14715**		
N/A	7/15/2020	4.6	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 and prior to 6.1.12. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional	N/A	A-ORA-VM_V-100820/594

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. Note: The CVE-2020-14628 is applicable to Windows VM only. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2020-14628**		
N/A	7/15/2020	4.9	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 and prior to 6.1.12. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0	N/A	A-ORA-VM_V-100820/595

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N). **CVE ID : CVE-2020-14629**		
N/A	7/15/2020	4.7	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 and prior to 6.1.12. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N). **CVE ID : CVE-2020-14673**	N/A	A-ORA-VM_V-100820/596
Time-of-check Time-of-use (TOCTOU)	7/15/2020	4.4	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization	N/A	A-ORA-VM_V-100820/597

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Race Condition			(component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 and prior to 6.1.12. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2020-14674**		
Time-of-check Time-of-use (TOCTOU) Race Condition	7/15/2020	4.4	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 and prior to 6.1.12. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise	N/A	A-ORA-VM_V-100820/598

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2020-14675**		
Out-of-bounds Read	7/15/2020	4.4	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 and prior to 6.1.12. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity	N/A	A-ORA-VM_V-100820/599

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2020-14676**		
Time-of-check Time-of-use (TOCTOU) Race Condition	7/15/2020	4.4	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 and prior to 6.1.12. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2020-14677**	N/A	A-ORA-VM_V-100820/600
transportation_management					
Information Exposure	7/15/2020	4	Vulnerability in the Oracle Transportation Management product of Oracle Supply Chain	N/A	A-ORA-TRAN-100820/601

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(component: Data, Domain & Function Security). The supported version that is affected is 6.4.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Transportation Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Transportation Management accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2020-14544**		
primavera_p6_enterprise_project_portfolio_management					
N/A	7/15/2020	5.5	Vulnerability in the Primavera P6 Enterprise Project Portfolio Management product of Oracle Construction and Engineering (component: Web Access). Supported versions that are affected are 16.1.0.0-16.2.20.1, 17.1.0.0-17.12.17.1 and 18.1.0.0-18.8.18.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Primavera P6 Enterprise Project	N/A	A-ORA-PRIM-100820/602

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Portfolio Management. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Primavera P6 Enterprise Project Portfolio Management accessible data as well as unauthorized read access to a subset of Primavera P6 Enterprise Project Portfolio Management accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2020-14653**		
N/A	7/15/2020	4	Vulnerability in the Primavera P6 Enterprise Project Portfolio Management product of Oracle Construction and Engineering (component: Web Access). Supported versions that are affected are 17.1.0.0-17.12.17.1, 18.1.0.0-18.8.19 and 19.12.0-19.12.5. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Primavera P6 Enterprise Project Portfolio Management. Successful attacks require human interaction from a person	N/A	A-ORA-PRIM-100820/603

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Primavera P6 Enterprise Project Portfolio Management accessible data as well as unauthorized update, insert or delete access to some of Primavera P6 Enterprise Project Portfolio Management accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:L/A:N). **CVE ID : CVE-2020-14706**		
database_server					
N/A	7/15/2020	4.6	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with network access via multiple protocols to compromise Java VM. Successful attacks require human interaction from a person other than the	N/A	A-ORA-DATA-100820/604

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker and while the vulnerability is in Java VM, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java VM. CVSS 3.1 Base Score 8.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2020-2968**		
N/A	7/15/2020	6	Vulnerability in the Data Pump component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows high privileged attacker having DBA role account privilege with network access via Oracle Net to compromise Data Pump. Successful attacks of this vulnerability can result in takeover of Data Pump. CVSS 3.1 Base Score 6.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2020-2969**	N/A	A-ORA-DATA-100820/605
configurator					
N/A	7/15/2020	5.8	Vulnerability in the Oracle Configurator product of Oracle Supply Chain	N/A	A-ORA-CONF-100820/606

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(component: UI Servlet). Supported versions that are affected are 12.1 and 12.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Configurator. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Configurator, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Configurator accessible data as well as unauthorized update, insert or delete access to some of Oracle Configurator accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2020-14669**		
webcenter_sites					
Improper Neutralization of Input During Web Page	7/15/2020	4.3	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component:	N/A	A-ORA-WEBC-100820/607

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Advanced User Interface). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Sites, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebCenter Sites accessible data as well as unauthorized read access to a subset of Oracle WebCenter Sites accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2020-14613**		
business_intelligence_publisher					
N/A	7/15/2020	6.4	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: Layout Templates). Supported	N/A	A-ORA-BUSI-100820/608

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions that are affected are 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle BI Publisher. While the vulnerability is in Oracle BI Publisher, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle BI Publisher accessible data as well as unauthorized read access to a subset of Oracle BI Publisher accessible data. CVSS 3.1 Base Score 7.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N). **CVE ID : CVE-2020-14696**		
peoplesoft_enterprise_human_capital_management_candidate_gateway					
N/A	7/15/2020	5.5	Vulnerability in the PeopleSoft Enterprise HRMS product of Oracle PeopleSoft (component: Time and Labor). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged	N/A	A-ORA-PEOP-100820/609

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker with network access via HTTP to compromise PeopleSoft Enterprise HRMS. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise HRMS accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise HRMS accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2020-14612**		
email_center					
N/A	7/15/2020	5.8	Vulnerability in the Oracle Email Center product of Oracle E-Business Suite (component: Message Display). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Email Center. Successful attacks require human interaction from a person other than the attacker and while the	N/A	A-ORA-EMAI-100820/610

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is in Oracle Email Center, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Email Center accessible data as well as unauthorized update, insert or delete access to some of Oracle Email Center accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2020-14666**		
marketing					
N/A	7/15/2020	4.3	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Marketing Administration). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the	N/A	A-ORA-MARK-100820/611

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.1 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N). **CVE ID : CVE-2020-14555**		
N/A	7/15/2020	6.4	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Marketing Administration). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Marketing accessible data as well as unauthorized access to critical data or complete access to all Oracle Marketing accessible data. CVSS 3.1 Base Score 9.1	N/A	A-ORA-MARK-100820/612

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2020-14658**		
business_intelligence					
Information Exposure	7/15/2020	2.1	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Web General). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 3.4 (Confidentiality impacts).	N/A	A-ORA-BUSI-100820/613

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		🟩	CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N). **CVE ID : CVE-2020-14548**		
N/A	7/15/2020	5.8	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Actions). Supported versions that are affected are 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized update, insert or delete access to some of Oracle Business	N/A	A-ORA-BUSI-100820/614

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2020-14690**		
N/A	7/15/2020	7.5	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Web Answers). Supported versions that are affected are 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data and unauthorized ability to cause a partial denial of	N/A	A-ORA-BUSI-100820/615

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (partial DOS) of Oracle Business Intelligence Enterprise Edition. CVSS 3.1 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L). **CVE ID : CVE-2020-14609**		
N/A	7/15/2020	6.8	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Web General). Supported versions that are affected are 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in takeover of Oracle Business Intelligence Enterprise Edition. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2020-14626**	N/A	A-ORA-BUSI-100820/616
application_object_library					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	7/15/2020	4.3	Vulnerability in the Oracle Application Object Library product of Oracle E-Business Suite (component: Diagnostics). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Application Object Library. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Object Library, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Object Library accessible data. CVSS 3.1 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N). **CVE ID : CVE-2020-14554**	N/A	A-ORA-APPL-100820/617
Information Exposure	7/15/2020	5	Vulnerability in the Oracle Application Object Library product of Oracle E-Business Suite (component: Logging). Supported versions that are affected are 12.2.5-	N/A	A-ORA-APPL-100820/618

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Application Object Library. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Application Object Library accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2020-14635**		
crm_technical_foundation					
N/A	7/15/2020	4.9	Vulnerability in the Oracle CRM Technical Foundation product of Oracle E-Business Suite (component: Preferences). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may	N/A	A-ORA-CRM_-100820/619

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle CRM Technical Foundation accessible data as well as unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2020-14657**		
N/A	7/15/2020	4.3	Vulnerability in the Oracle CRM Technical Foundation product of Oracle E-Business Suite (component: Preferences). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical	N/A	A-ORA-CRM_-100820/620

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.1 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N). **CVE ID : CVE-2020-14659**		
N/A	7/15/2020	5.8	Vulnerability in the Oracle CRM Technical Foundation product of Oracle E-Business Suite (component: Preferences). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to	N/A	A-ORA-CRM_-100820/621

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			critical data or complete access to all Oracle CRM Technical Foundation accessible data as well as unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2020-14660**		
N/A	7/15/2020	4.3	Vulnerability in the Oracle CRM Technical Foundation product of Oracle E-Business Suite (component: Preferences). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in	N/A	A-ORA-CRM_-100820/622

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.1 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N). **CVE ID : CVE-2020-14661**		
N/A	7/15/2020	4.9	Vulnerability in the Oracle CRM Technical Foundation product of Oracle E-Business Suite (component: Preferences). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle CRM Technical Foundation accessible data as well as unauthorized update,	N/A	A-ORA-CRM_-100820/623

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2020-14667**		
N/A	7/15/2020	5	Vulnerability in the Oracle CRM Technical Foundation product of Oracle E-Business Suite (component: Preferences). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle CRM Technical Foundation. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14679**	N/A	A-ORA-CRM_-100820/624
trade_management					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	7/15/2020	6.4	Vulnerability in the Oracle Trade Management product of Oracle E-Business Suite (component: Invoice). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Trade Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Trade Management accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2020-14665**	N/A	A-ORA-TRAD-100820/625
istore					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/15/2020	4.3	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: User Registration). Supported versions that are affected are 12.1.1-12.1.3 and	N/A	A-ORA-ISTO-100820/626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2020-14582**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/15/2020	4.3	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Address Book). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network	N/A	A-ORA-ISTO-100820/627

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2020-14596**		
commerce_platform					
N/A	7/15/2020	4.3	Vulnerability in the Oracle Commerce Platform product of Oracle Commerce (component: Dynamo Application Framework). Supported versions that are affected are 11.1, 11.2 and prior to 11.3.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via	N/A	A-ORA-COMM-100820/628

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HTTP to compromise Oracle Commerce Platform. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Platform, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Commerce Platform accessible data. CVSS 3.1 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N). **CVE ID : CVE-2020-14532**		
N/A	7/15/2020	4.9	Vulnerability in the Oracle Commerce Platform product of Oracle Commerce (component: Dynamo Application Framework). Supported versions that are affected are 11.1, 11.2 and prior to 11.3.1. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Commerce Platform. Successful attacks require human interaction from a person other than the attacker. Successful attacks	N/A	A-ORA-COMM-100820/629

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Commerce Platform accessible data as well as unauthorized read access to a subset of Oracle Commerce Platform accessible data. CVSS 3.1 Base Score 3.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:N). **CVE ID : CVE-2020-14533**		
advanced_outbound_telephony					
N/A	7/15/2020	5.8	Vulnerability in the Oracle Advanced Outbound Telephony product of Oracle E-Business Suite (component: Settings). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Advanced Outbound Telephony. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Advanced Outbound Telephony, attacks may	N/A	A-ORA-ADVA-100820/630

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Advanced Outbound Telephony accessible data as well as unauthorized update, insert or delete access to some of Oracle Advanced Outbound Telephony accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2020-14670**		
N/A	7/15/2020	5.8	Vulnerability in the Oracle Advanced Outbound Telephony product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Advanced Outbound Telephony. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Advanced	N/A	A-ORA-ADVA-100820/631

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Outbound Telephony, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Advanced Outbound Telephony accessible data as well as unauthorized update, insert or delete access to some of Oracle Advanced Outbound Telephony accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR: N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2020-14671**		
common_applications					
N/A	7/15/2020	4.3	Vulnerability in the Oracle Common Applications product of Oracle E-Business Suite (component: CRM User Management Framework). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Common Applications. Successful attacks require	N/A	A-ORA-COMM-100820/632

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			human interaction from a person other than the attacker and while the vulnerability is in Oracle Common Applications, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Common Applications accessible data. CVSS 3.1 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N). **CVE ID : CVE-2020-14716**		
N/A	7/15/2020	4.3	Vulnerability in the Oracle Common Applications product of Oracle E-Business Suite (component: CRM User Management Framework). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Common Applications. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Common Applications, attacks may significantly	N/A	A-ORA-COMM-100820/633

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Common Applications accessible data. CVSS 3.1 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N). **CVE ID : CVE-2020-14717**		
N/A	7/15/2020	5.8	Vulnerability in the Oracle Common Applications product of Oracle E-Business Suite (component: CRM User Management Framework). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Common Applications. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Common Applications, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all	N/A	A-ORA-COMM-100820/634

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle Common Applications accessible data as well as unauthorized update, insert or delete access to some of Oracle Common Applications accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2020-14688**		
applications_framework					
N/A	7/15/2020	5.8	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Popups). The supported version that is affected is 12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Applications Framework, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or	N/A	A-ORA-APPL-100820/635

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			complete access to all Oracle Applications Framework accessible data as well as unauthorized update, insert or delete access to some of Oracle Applications Framework accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2020-14534**		
N/A	7/15/2020	4	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Page Request). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Applications Framework. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Applications Framework accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).	N/A	A-ORA-APPL-100820/636

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14590		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/15/2020	3.5	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Attachments / File Upload). The supported version that is affected is 12.2.9. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Applications Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Applications Framework, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Applications Framework accessible data as well as unauthorized update, insert or delete access to some of Oracle Applications Framework accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N).	N/A	A-ORA-APPL-100820/637

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14610		
hyperion_financial_close_management					
N/A	7/15/2020	2.1	Vulnerability in the Hyperion Financial Close Management product of Oracle Hyperion (component: Close Manager). The supported version that is affected is 11.1.2.4. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Hyperion Financial Close Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Hyperion Financial Close Management accessible data. CVSS 3.1 Base Score 2.0 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:N). **CVE ID : CVE-2020-14541**	N/A	A-ORA-HYPE-100820/638
N/A	7/15/2020	2.1	Vulnerability in the Hyperion Financial Close Management product of Oracle Hyperion (component: Close Manager). The supported version that is affected is 11.1.2.4. Difficult to exploit	N/A	A-ORA-HYPE-100820/639

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows high privileged attacker with network access via HTTP to compromise Hyperion Financial Close Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Hyperion Financial Close Management accessible data. CVSS 3.1 Base Score 4.2 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:H/A:N). **CVE ID : CVE-2020-14546**		
primavera_portfolio_management					
N/A	7/15/2020	4	Vulnerability in the Primavera Portfolio Management product of Oracle Construction and Engineering (component: Web Server). Supported versions that are affected are 16.1.0.0-16.1.5.1, 18.0.0.0-18.0.2.0 and 19.0.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Primavera Portfolio Management. Successful attacks require human	N/A	A-ORA-PRIM-100820/640

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Primavera Portfolio Management accessible data as well as unauthorized update, insert or delete access to some of Primavera Portfolio Management accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:L/A:N). **CVE ID : CVE-2020-14549**		
N/A	7/15/2020	4.3	Vulnerability in the Primavera Portfolio Management product of Oracle Construction and Engineering (component: Web Access). Supported versions that are affected are 16.1.0.0-16.1.5.1, 18.0.0.0-18.0.2.0 and 19.0.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Primavera Portfolio Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this	N/A	A-ORA-PRIM-100820/641

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can result in unauthorized update, insert or delete access to some of Primavera Portfolio Management accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N). **CVE ID : CVE-2020-14566**		
N/A	7/15/2020	4	Vulnerability in the Primavera Portfolio Management product of Oracle Construction and Engineering (component: Web Access). Supported versions that are affected are 16.1.0.0-16.1.5.1, 18.0.0.0-18.0.2.0 and 19.0.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Primavera Portfolio Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Primavera Portfolio Management accessible data as well as unauthorized update, insert or delete access to some of Primavera Portfolio Management	N/A	A-ORA-PRIM-100820/642

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:L/A:N). **CVE ID : CVE-2020-14527**		
N/A	7/15/2020	5.8	Vulnerability in the Primavera Portfolio Management product of Oracle Construction and Engineering (component: Web Access). Supported versions that are affected are 16.1.0.0-16.1.5.1, 18.0.0.0-18.0.2.0 and 19.0.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Primavera Portfolio Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Primavera Portfolio Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Primavera Portfolio Management accessible data as well as unauthorized read access to a subset of Primavera	N/A	A-ORA-PRIM-100820/643

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Portfolio Management accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2020-14528**		
N/A	7/15/2020	4.9	Vulnerability in the Primavera Portfolio Management product of Oracle Construction and Engineering (component: Investor Module). Supported versions that are affected are 16.1.0.0-16.1.5.1, 18.0.0.0-18.0.2.0 and 19.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Primavera Portfolio Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Primavera Portfolio Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Primavera Portfolio Management accessible data as well as	N/A	A-ORA-PRIM-100820/644

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized read access to a subset of Primavera Portfolio Management accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2020-14529**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/15/2020	4.3	Vulnerability in the Primavera Portfolio Management product of Oracle Construction and Engineering (component: Investor Module). Supported versions that are affected are 16.1.0.0-16.1.5.1, 18.0.0.0-18.0.2.0 and 19.0.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Primavera Portfolio Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Primavera Portfolio Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Primavera	N/A	A-ORA-PRIM-100820/645

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Portfolio Management accessible data as well as unauthorized read access to a subset of Primavera Portfolio Management accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2020-2562**		
communications_interactive_session_recorder					
N/A	7/15/2020	3	Vulnerability in the Oracle Communications Interactive Session Recorder product of Oracle Communications Applications (component: FACE). Supported versions that are affected are 6.1-6.4. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Communications Interactive Session Recorder executes to compromise Oracle Communications Interactive Session Recorder. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Communications Interactive Session	N/A	A-ORA-COMM-100820/646

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Recorder accessible data as well as unauthorized update, insert or delete access to some of Oracle Communications Interactive Session Recorder accessible data. CVSS 3.1 Base Score 4.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:L/A:N). **CVE ID : CVE-2020-14574**		
communications_applications					
N/A	7/15/2020	6	Vulnerability in the Oracle Communications Session Border Controller product of Oracle Communications Applications (component: System Admin). Supported versions that are affected are 8.1.0, 8.2.0 and 8.3.0. Easily exploitable vulnerability allows low privileged attacker with network access via SSH to compromise Oracle Communications Session Border Controller. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Communications Session Border Controller, attacks may significantly impact additional products. Successful attacks of this	N/A	A-ORA-COMM-100820/647

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can result in unauthorized access to critical data or complete access to all Oracle Communications Session Border Controller accessible data as well as unauthorized update, insert or delete access to some of Oracle Communications Session Border Controller accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Communications Session Border Controller. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:L). **CVE ID : CVE-2020-14580**		
peoplesoft_products					
N/A	7/15/2020	5.5	Vulnerability in the PeopleSoft Enterprise FIN Expenses product of Oracle PeopleSoft (component: Expenses). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise FIN Expenses. Successful attacks of this vulnerability can result in	N/A	A-ORA-PEOP-100820/648

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized update, insert or delete access to some of PeopleSoft Enterprise FIN Expenses accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise FIN Expenses accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2020-14587**		
sd-wan_edge					
N/A	7/15/2020	10	Vulnerability in the Oracle SD-WAN Edge product of Oracle Communications Applications (component: User Interface). Supported versions that are affected are 8.2 and 9.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle SD-WAN Edge. While the vulnerability is in Oracle SD-WAN Edge, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle SD-WAN Edge. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability	N/A	A-ORA-SD-W-100820/649

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2020-14606**		
fusion_middleware_mapviewer					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/15/2020	4.3	Vulnerability in the Oracle Fusion Middleware MapViewer product of Oracle Fusion Middleware (component: Tile Server). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Fusion Middleware MapViewer. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Fusion Middleware MapViewer, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Fusion Middleware MapViewer accessible data as well as unauthorized read access to a subset of Oracle Fusion Middleware MapViewer accessible data. CVSS 3.1 Base Score	N/A	A-ORA-FUSI-100820/650

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2020-14607**		
N/A	7/15/2020	6.4	Vulnerability in the Oracle Fusion Middleware MapViewer product of Oracle Fusion Middleware (component: Tile Server). The supported version that is affected is 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Fusion Middleware MapViewer. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Fusion Middleware MapViewer accessible data as well as unauthorized read access to a subset of Oracle Fusion Middleware MapViewer accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N). **CVE ID : CVE-2020-14608**	N/A	A-ORA-FUSI-100820/651
security_service					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	7/15/2020	5.8	Vulnerability in the Oracle Security Service product of Oracle Fusion Middleware (component: SSL API). Supported versions that are affected are 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Security Service. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Security Service accessible data as well as unauthorized update, insert or delete access to some of Oracle Security Service accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N). **CVE ID : CVE-2020-14655**	N/A	A-ORA-SECU-100820/652
N/A	7/15/2020	4.3	Vulnerability in the Oracle Security Service product of Oracle Fusion Middleware (component: None). The supported version that is affected is 11.1.1.9.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via	N/A	A-ORA-SECU-100820/653

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HTTPS to compromise Oracle Security Service. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Security Service accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2020-14530**		
commerce_service_center					
N/A	7/15/2020	5.8	Vulnerability in the Oracle Commerce Service Center product of Oracle Commerce (component: Commerce Service Center). Supported versions that are affected are 11.1, 11.2 and prior to 11.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Service Center. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Commerce Service Center accessible data as well as unauthorized access to critical data or complete access to all Oracle	N/A	A-ORA-COMM-100820/654

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Commerce Service Center accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2020-14535**		
commerce_experience_manager					
N/A	7/15/2020	5.8	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Workbench). Supported versions that are affected are 11.0, 11.1, 11.2 and prior to 11.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data as well as unauthorized access to critical data or complete access to all Oracle Commerce Guided Search /	N/A	A-ORA-COMM-100820/655

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2020-14536**		
commerce_guided_search					
N/A	7/15/2020	5.8	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Workbench). Supported versions that are affected are 11.0, 11.1, 11.2 and prior to 11.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data as well as unauthorized access to critical data or complete access to all Oracle	N/A	A-ORA-COMM-100820/656

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2020-14536**		
enterprise_communications_broker					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/15/2020	4.3	Vulnerability in the Oracle Enterprise Communications Broker product of Oracle Communications Applications (component: WebGUI). Supported versions that are affected are 3.0.0-3.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Enterprise Communications Broker. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Enterprise Communications Broker, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized	N/A	A-ORA-ENTE-100820/657

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			update, insert or delete access to some of Oracle Enterprise Communications Broker accessible data as well as unauthorized read access to a subset of Oracle Enterprise Communications Broker accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2020-14563**		
N/A	7/15/2020	6.5	Vulnerability in the Oracle Enterprise Communications Broker product of Oracle Communications Applications (component: WebGUI). Supported versions that are affected are 3.0.0-3.2.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Communications Broker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Enterprise Communications Broker accessible data as well as unauthorized read access	N/A	A-ORA-ENTE-100820/658

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to a subset of Oracle Enterprise Communications Broker accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Enterprise Communications Broker. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L). **CVE ID : CVE-2020-14721**		
N/A	7/15/2020	5.1	Vulnerability in the Oracle Enterprise Communications Broker product of Oracle Communications Applications (component: WebGUI). Supported versions that are affected are 3.0.0-3.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Enterprise Communications Broker. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Enterprise Communications Broker, attacks may significantly impact additional products. Successful	N/A	A-ORA-ENTE-100820/659

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Enterprise Communications Broker accessible data as well as unauthorized read access to a subset of Oracle Enterprise Communications Broker accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Enterprise Communications Broker. CVSS 3.1 Base Score 5.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:L). **CVE ID : CVE-2020-14722**		
unified_directory					
N/A	7/15/2020	4.9	Vulnerability in the Oracle Unified Directory product of Oracle Fusion Middleware (component: Security). Supported versions that are affected are 11.1.2.3.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Unified Directory. Successful attacks require human	N/A	A-ORA-UNIF-100820/660

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction from a person other than the attacker and while the vulnerability is in Oracle Unified Directory, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Unified Directory accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Unified Directory. CVSS 3.1 Base Score 8.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR: H/UI:R/S:C/C:N/I:H/A:H). **CVE ID : CVE-2020-14565**		
primavera_unifier					
N/A	7/15/2020	3.5	Vulnerability in the Primavera Unifier product of Oracle Construction and Engineering (component: Platform, Mobile App). Supported versions that are affected are 16.1, 16.2, 17.7-17.12, 18.8 and 19.12; Mobile App: Prior to 20.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Primavera	N/A	A-ORA-PRIM-100820/661

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Unifier. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Primavera Unifier accessible data. CVSS 3.1 Base Score 5.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N). **CVE ID : CVE-2020-14617**		
N/A	7/15/2020	4	Vulnerability in the Primavera Unifier product of Oracle Construction and Engineering (component: Mobile App). The supported version that is affected is Prior to 20.6. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Primavera Unifier. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Primavera Unifier accessible data as well as unauthorized update, insert or delete access to	N/A	A-ORA-PRIM-100820/662

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			some of Primavera Unifier accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:L/A:N). **CVE ID : CVE-2020-14618**		
enterprise_session_border_controller					
Improper Resource Shutdown or Release	7/15/2020	7.5	Vulnerability in the Oracle Enterprise Session Border Controller product of Oracle Communications Applications (component: File Upload). Supported versions that are affected are 8.1.0, 8.2.0 and 8.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Enterprise Session Border Controller. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Enterprise Session Border Controller, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Enterprise Session Border Controller	N/A	A-ORA-ENTE-100820/663

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			as well as unauthorized update, insert or delete access to some of Oracle Enterprise Session Border Controller accessible data and unauthorized read access to a subset of Oracle Enterprise Session Border Controller accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:H). **CVE ID : CVE-2020-14630**		
sd-wan_aware					
N/A	7/15/2020	7.5	Vulnerability in the Oracle SD-WAN Aware product of Oracle Communications Applications (component: User Interface). The supported version that is affected is 8.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle SD-WAN Aware. While the vulnerability is in Oracle SD-WAN Aware, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle SD-WAN Aware. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability	N/A	A-ORA-SD-W-100820/664

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2020-14701**		
goldengate					
N/A	7/15/2020	5.8	Vulnerability in the Oracle GoldenGate product of Oracle GoldenGate (component: Process Management). The supported version that is affected is Prior to 19.1.0.0.0. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle GoldenGate executes to compromise Oracle GoldenGate. While the vulnerability is in Oracle GoldenGate, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle GoldenGate. CVSS 3.1 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2020-14705**	N/A	A-ORA-GOLD-100820/665
internet_expenses					
N/A	7/15/2020	4	Vulnerability in the Oracle Internet Expenses product	N/A	A-ORA-INTE-100820/666

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of Oracle E-Business Suite (component: Mobile Expenses Admin Utilities). Supported versions that are affected are 12.2.4-12.2.9. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Internet Expenses. While the vulnerability is in Oracle Internet Expenses, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Internet Expenses accessible data. CVSS 3.1 Base Score 7.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:N). **CVE ID : CVE-2020-14719**		
N/A	7/15/2020	4	Vulnerability in the Oracle Internet Expenses product of Oracle E-Business Suite (component: Mobile Expenses Admin Utilities). Supported versions that are affected are 12.2.4-12.2.9. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Internet Expenses. While	N/A	A-ORA-INTE-100820/667

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the vulnerability is in Oracle Internet Expenses, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Internet Expenses accessible data. CVSS 3.1 Base Score 7.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N). **CVE ID : CVE-2020-14720**		
help_technologies					
N/A	7/15/2020	5.8	Vulnerability in the Oracle Help Technologies product of Oracle Fusion Middleware (component: Web UIX). Supported versions that are affected are 11.1.1.9.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Help Technologies. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Help Technologies, attacks may significantly impact additional products. Successful	N/A	A-ORA-HELP-100820/668

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Help Technologies accessible data as well as unauthorized update, insert or delete access to some of Oracle Help Technologies accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2020-14723**		
hyperion_bi\+					
N/A	7/15/2020	2.1	Vulnerability in the Oracle Hyperion BI+ product of Oracle Hyperion (component: UI and Visualization). The supported version that is affected is 11.1.2.4. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Hyperion BI+. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion BI+ accessible	N/A	A-ORA-HYPE-100820/669

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			data. CVSS 3.1 Base Score 4.2 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:N/A:N). **CVE ID : CVE-2020-14560**		
berkeley_db					
N/A	7/15/2020	3.7	Vulnerability in the Data Store component of Oracle Berkeley DB. The supported version that is affected is Prior to 18.1.40. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Data Store executes to compromise Data Store. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Data Store. CVSS 3.1 Base Score 7.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2020-2981**	N/A	A-ORA-BERK-100820/670
flexcube_investor_servicing					
N/A	7/15/2020	5.5	Vulnerability in the Oracle FLEXCUBE Investor Servicing product of Oracle Financial Services Applications (component: Infrastructure). Supported	N/A	A-ORA-FLEX-100820/671

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions that are affected are 12.1.0, 12.3.0, 12.4.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Investor Servicing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle FLEXCUBE Investor Servicing accessible data as well as unauthorized access to critical data or complete access to all Oracle FLEXCUBE Investor Servicing accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2020-14569**		
food_and_beverage_applications					
N/A	7/15/2020	4.4	Vulnerability in the Oracle Hospitality Reporting and Analytics product of Oracle Food and Beverage Applications (component: Installation). The supported version that is affected is 9.1.0. Easily exploitable vulnerability allows low privileged	N/A	A-ORA-FOOD-100820/672

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker with logon to the infrastructure where Oracle Hospitality Reporting and Analytics executes to compromise Oracle Hospitality Reporting and Analytics. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Hospitality Reporting and Analytics. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2020-14561**		
N/A	7/15/2020	4.4	Vulnerability in the Oracle Hospitality Reporting and Analytics product of Oracle Food and Beverage Applications (component: Inventory Integration). The supported version that is affected is 9.1.0. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Hospitality Reporting and Analytics executes to compromise Oracle Hospitality Reporting and Analytics. Successful attacks require human interaction from a person other than the	N/A	A-ORA-FOOD-100820/673

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker. Successful attacks of this vulnerability can result in takeover of Oracle Hospitality Reporting and Analytics. CVSS 3.1 Base Score 6.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2020-14594**		
N/A	7/15/2020	4	Vulnerability in the Oracle Hospitality Reporting and Analytics product of Oracle Food and Beverage Applications (component: Reporting). The supported version that is affected is 9.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Hospitality Reporting and Analytics. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hospitality Reporting and Analytics accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2020-14616**	N/A	A-ORA-FOOD-100820/674
bi_publisher					
N/A	7/15/2020	5.8	Vulnerability in the Oracle BI Publisher product of	N/A	A-ORA-BI_P-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle Fusion Middleware (component: Mobile Service). Supported versions that are affected are 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle BI Publisher accessible data as well as unauthorized update, insert or delete access to some of Oracle BI Publisher accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:N). **CVE ID : CVE-2020-14570**		100820/675
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	7/15/2020	6.4	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: Mobile Service). Supported versions that are affected are 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability	N/A	A-ORA-BI_P-100820/676

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows unauthenticated attacker with network access via HTTP to compromise Oracle BI Publisher. While the vulnerability is in Oracle BI Publisher, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle BI Publisher accessible data as well as unauthorized read access to a subset of Oracle BI Publisher accessible data. CVSS 3.1 Base Score 7.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N). **CVE ID : CVE-2020-14571**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/15/2020	4.3	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: BI Publisher Security). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks require human	N/A	A-ORA-BI_P-100820/677

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction from a person other than the attacker and while the vulnerability is in Oracle BI Publisher, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle BI Publisher accessible data as well as unauthorized update, insert or delete access to some of Oracle BI Publisher accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2020-14584**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/15/2020	4.3	Vulnerability in the Oracle BI Publisher product of Oracle Fusion Middleware (component: Mobile Service). Supported versions that are affected are 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks require human interaction from a person other than the attacker and	N/A	A-ORA-BI_P-100820/678

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			while the vulnerability is in Oracle BI Publisher, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle BI Publisher accessible data as well as unauthorized update, insert or delete access to some of Oracle BI Publisher accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2020-14585**		
graalvm					
N/A	7/15/2020	6.5	Vulnerability in the Oracle GraalVM Enterprise Edition product of Oracle GraalVM (component: JVMCI). Supported versions that are affected are 19.3.2 and 20.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in takeover of Oracle	N/A	A-ORA-GRAA-100820/679

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			GraalVM Enterprise Edition. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2020-14718**		
financial_services_analytical_applications_infrastructure					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/15/2020	4.3	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 8.0.6-8.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Financial Services Analytical Applications Infrastructure, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial	N/A	A-ORA-FINA-100820/680

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Services Analytical Applications Infrastructure accessible data as well as unauthorized read access to a subset of Oracle Financial Services Analytical Applications Infrastructure accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2020-14601**		
N/A	7/15/2020	5.5	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 8.0.6-8.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financial Services Analytical Applications Infrastructure accessible data as well as	N/A	A-ORA-FINA-100820/681

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized read access to a subset of Oracle Financial Services Analytical Applications Infrastructure accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N). **CVE ID : CVE-2020-14602**		
N/A	7/15/2020	5	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 8.0.6-8.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Financial Services Analytical Applications Infrastructure accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	N/A	A-ORA-FINA-100820/682

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14603		
N/A	7/15/2020	5	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 8.0.6-8.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Financial Services Analytical Applications Infrastructure accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2020-14604**	N/A	A-ORA-FINA-100820/683
N/A	7/15/2020	4	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 8.0.6-8.1.0. Easily exploitable vulnerability	N/A	A-ORA-FINA-100820/684

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financial Services Analytical Applications Infrastructure accessible data. CVSS 3.1 Base Score 6.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2020-14605**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/15/2020	4.3	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 8.0.6-8.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks require human interaction from a person other than the attacker and	N/A	A-ORA-FINA-100820/685

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			while the vulnerability is in Oracle Financial Services Analytical Applications Infrastructure, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Analytical Applications Infrastructure accessible data as well as unauthorized read access to a subset of Oracle Financial Services Analytical Applications Infrastructure accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2020-14615**		
N/A	7/15/2020	6.5	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 8.0.6-8.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services	N/A	A-ORA-FINA-100820/686

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Analytical Applications Infrastructure. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Analytical Applications Infrastructure accessible data as well as unauthorized read access to a subset of Oracle Financial Services Analytical Applications Infrastructure accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Financial Services Analytical Applications Infrastructure. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L). **CVE ID : CVE-2020-14662**		
N/A	7/15/2020	4.3	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 8.0.6-8.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network	N/A	A-ORA-FINA-100820/687

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Analytical Applications Infrastructure accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N). **CVE ID : CVE-2020-14684**		
N/A	7/15/2020	4	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 8.0.6-8.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks of this vulnerability can result in unauthorized creation, deletion or	N/A	A-ORA-FINA-100820/688

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			modification access to critical data or all Oracle Financial Services Analytical Applications Infrastructure accessible data. CVSS 3.1 Base Score 6.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2020-14685**		
isupport					
N/A	7/15/2020	5.8	Vulnerability in the Oracle iSupport product of Oracle E-Business Suite (component: Others). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iSupport. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iSupport, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iSupport accessible data as well as unauthorized update, insert or delete	N/A	A-ORA-ISUP-100820/689

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to some of Oracle iSupport accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2020-14686**		
siebel_ui_framework					
N/A	7/15/2020	4	Vulnerability in the Siebel UI Framework product of Oracle Siebel CRM (component: SWSE Server). Supported versions that are affected are 20.6 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel UI Framework. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Siebel UI Framework accessible data as well as unauthorized update, insert or delete access to some of Siebel UI Framework accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality and Integrity impacts). CVSS Vector:	N/A	A-ORA-SIEB-100820/690

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:L/A:N). **CVE ID : CVE-2020-14531**		
data_masking_and_subsetting					
N/A	7/15/2020	5.5	Vulnerability in the Oracle Data Masking and Subsetting product of Oracle Enterprise Manager (component: Data Masking). Supported versions that are affected are 13.3.0.0 and 13.4.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Data Masking and Subsetting. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Data Masking and Subsetting accessible data as well as unauthorized update, insert or delete access to some of Oracle Data Masking and Subsetting accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N). **CVE ID : CVE-2020-2983**	N/A	A-ORA-DATA-100820/691
configuration_manager					
N/A	7/15/2020	5.5	Vulnerability in the Oracle	N/A	A-ORA-CONF-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Configuration Manager product of Oracle Enterprise Manager (component: Discovery and collection script). The supported version that is affected is 12.1.2.0.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Configuration Manager. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Configuration Manager accessible data as well as unauthorized update, insert or delete access to some of Oracle Configuration Manager accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N). **CVE ID : CVE-2020-2984**		100820/692
weblogic_server					
N/A	7/15/2020	4	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Container). Supported versions that are affected are 12.1.3.0.0,	N/A	A-ORA-WEBL-100820/693

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebLogic Server accessible data as well as unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N). **CVE ID : CVE-2020-14557**		
Information Exposure	7/15/2020	5.8	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Sample apps). Supported versions that are affected are 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker	N/A	A-ORA-WEBL-100820/694

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2020-14636**		
N/A	7/15/2020	5.8	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Sample apps). Supported versions that are affected are 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise	N/A	A-ORA-WEBL-100820/695

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2020-14637**		
N/A	7/15/2020	5.8	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Sample apps). Supported versions that are affected are 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require	N/A	A-ORA-WEBL-100820/696

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2020-14638**		
Information Exposure	7/15/2020	5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Sample apps). Supported versions that are affected are 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to	N/A	A-ORA-WEBL-100820/697

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2020-14639**		
N/A	7/15/2020	5.8	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Sample apps). Supported versions that are affected are 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server	N/A	A-ORA-WEBL-100820/698

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2020-14640**		
N/A	7/15/2020	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2020-14644**	N/A	A-ORA-WEBL-100820/699
N/A	7/15/2020	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0,	N/A	A-ORA-WEBL-100820/700

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2020-14645**		
N/A	7/15/2020	6.4	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read	N/A	A-ORA-WEBL-100820/701

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2020-14652**		
N/A	7/15/2020	5.8	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS	N/A	A-ORA-WEBL-100820/702

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N). **CVE ID : CVE-2020-2966**		
N/A	7/15/2020	5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2020-2967**	N/A	A-ORA-WEBL-100820/703
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/15/2020	4.3	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0.	N/A	A-ORA-WEBL-100820/704

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2020-14572**		
N/A	7/15/2020	6.4	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Container). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable	N/A	A-ORA-WEBL-100820/705

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N). **CVE ID : CVE-2020-14588**		
N/A	7/15/2020	5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Container). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to	N/A	A-ORA-WEBL-100820/706

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14589**		
N/A	7/15/2020	4	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2020-14622**	N/A	A-ORA-WEBL-100820/707
N/A	7/15/2020	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion	N/A	A-ORA-WEBL-100820/708

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2020-14625**		
N/A	7/15/2020	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8	N/A	A-ORA-WEBL-100820/709

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2020-14687**		
hospitality_reporting_and_analytics					
N/A	7/15/2020	4.4	Vulnerability in the Oracle Hospitality Reporting and Analytics product of Oracle Food and Beverage Applications (component: Installation). The supported version that is affected is 9.1.0. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hospitality Reporting and Analytics executes to compromise Oracle Hospitality Reporting and Analytics. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Hospitality Reporting and Analytics. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2020-14543**	N/A	A-ORA-HOSP-100820/710
peoplesoft_enterprise_peopletools					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	7/15/2020	5	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.56, 8.57 and 8.58. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2020-14558**	N/A	A-ORA-PEOP-100820/711
N/A	7/15/2020	5.8	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Environment Mgmt Console). Supported versions that are affected are 8.56, 8.57 and 8.58. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human	N/A	A-ORA-PEOP-100820/712

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of PeopleSoft Enterprise PeopleTools as well as unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 8.2 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:H). **CVE ID : CVE-2020-14564**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/15/2020	4.3	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Rich Text Editor). Supported versions that are affected are 8.56, 8.57 and 8.58. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful	N/A	A-ORA-PEOP-100820/713

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2020-14592**		
N/A	7/15/2020	4.3	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Portal). Supported versions that are affected are 8.56, 8.57 and 8.58. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human	N/A	A-ORA-PEOP-100820/714

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N). **CVE ID : CVE-2020-14600**		
N/A	7/15/2020	5.8	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Query). Supported versions that are affected are 8.56, 8.57 and 8.58. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft	N/A	A-ORA-PEOP-100820/715

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2020-14627**		
database					
N/A	7/15/2020	4	Vulnerability in the Oracle Database - Enterprise Edition component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows high privileged attacker having DBA role account privilege with network access via Oracle Net to compromise Oracle Database - Enterprise Edition. While the vulnerability is in Oracle Database - Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Database - Enterprise Edition	N/A	A-ORA-DATA-100820/716

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			accessible data. CVSS 3.1 Base Score 4.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:L/A:N). **CVE ID : CVE-2020-2978**		
Pandorafms					
pandora_fms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/13/2020	9.3	Pandora FMS 7.0 NG <= 746 suffers from Multiple XSS vulnerabilities in different browser views. A network administrator scanning a SNMP device can trigger a Cross Site Scripting (XSS), which can run arbitrary code to allow Remote Code Execution as root or apache2. **CVE ID : CVE-2020-11749**	https://pandorafms.com/downloads/whats-new-747-EN.pdf	A-PAN-PAND-100820/717
parall					
jspdf					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/6/2020	4.3	In all versions of package jspdf, it is possible to inject JavaScript code via the html method. **CVE ID : CVE-2020-7690**	N/A	A-PAR-JSPD-100820/718
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/6/2020	4.3	In all versions of the package jspdf, it is possible to use <<script>script> in order to go over the filtering regex. **CVE ID : CVE-2020-7691**	N/A	A-PAR-JSPD-100820/719
persian_vip_download_script_project					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
persian_vip_download_script					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	7/1/2020	7.5	Persian VIP Download Script 1.0 allows SQL Injection via the cart_edit.php active parameter. **CVE ID : CVE-2020-15468**	N/A	A-PER-PERS-100820/720
Phoenixcontact					
pc_worx					
Out-of-bounds Write	7/1/2020	6.8	PLCopen XML file parsing in Phoenix Contact PC Worx and PC Worx Express version 1.87 and earlier can lead to a stack-based overflow. Manipulated PC Worx projects could lead to a remote code execution due to insufficient input data validation. **CVE ID : CVE-2020-12497**	https://cert.vde.com/de-de/advisories/vde-2020-023	A-PHO-PC_W-100820/721
Out-of-bounds Read	7/1/2020	6.8	mwe file parsing in Phoenix Contact PC Worx and PC Worx Express version 1.87 and earlier is vulnerable to out-of-bounds read remote code execution. Manipulated PC Worx projects could lead to a remote code execution due to insufficient input data validation. **CVE ID : CVE-2020-12498**	https://cert.vde.com/de-de/advisories/vde-2020-023	A-PHO-PC_W-100820/722
pc_worx_express					
Out-of-bounds Write	7/1/2020	6.8	PLCopen XML file parsing in Phoenix Contact PC	https://cert.vde.com/d	A-PHO-PC_W-100820/723

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Worx and PC Worx Express version 1.87 and earlier can lead to a stack-based overflow. Manipulated PC Worx projects could lead to a remote code execution due to insufficient input data validation. **CVE ID : CVE-2020-12497**	e-de/advisories/vde-2020-023	
Out-of-bounds Read	7/1/2020	6.8	mwe file parsing in Phoenix Contact PC Worx and PC Worx Express version 1.87 and earlier is vulnerable to out-of-bounds read remote code execution. Manipulated PC Worx projects could lead to a remote code execution due to insufficient input data validation. **CVE ID : CVE-2020-12498**	https://cert.vde.com/de-de/advisories/vde-2020-023	A-PHO-PC_W-100820/724
Phplist					
phplist					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	7/8/2020	6.5	An issue was discovered in phpList through 3.5.4. An error-based SQL Injection vulnerability exists via the Import Administrators section. **CVE ID : CVE-2020-15072**	https://discuss.phplist.org/t/phplist-3-5-5-has-been-released/6377, https://www.phplist.org/newslist/phplist-3-5-5-release-notes/	A-PHP-PHPL-100820/725
Improper Neutralization	7/8/2020	3.5	An issue was discovered in phpList through 3.5.4. An	https://discuss.phplist.	A-PHP-PHPL-100820/726

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input During Web Page Generation ('Cross-site Scripting')			XSS vulnerability occurs within the Import Administrators section via upload of an edited text document. This also affects the Subscriber Lists section. **CVE ID : CVE-2020-15073**	org/t/phplist-3-5-5-has-been-released/6377, https://www.phplist.org/newslist/phplist-3-5-5-release-notes/	
phpzag					
phpzag					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	7/7/2020	7.5	SQL injection with the search parameter in Records.php for phpzag live add edit delete data tables records with ajax php mysql **CVE ID : CVE-2020-8519**	N/A	A-PHP-PHPZ-100820/727
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	7/7/2020	7.5	SQL injection in order and column parameters in Records.php for phpzag live add edit delete data tables records with ajax php mysql **CVE ID : CVE-2020-8520**	N/A	A-PHP-PHPZ-100820/728
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	7/7/2020	7.5	SQL injection with start and length parameters in Records.php for phpzag live add edit delete data tables records with ajax php mysql **CVE ID : CVE-2020-8521**	N/A	A-PHP-PHPZ-100820/729
Powerdns					
recursor					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	7/1/2020	4.3	In PowerDNS Recursor versions up to and including 4.3.1, 4.2.2 and 4.1.16, the ACL restricting access to the internal web server is not properly enforced. **CVE ID : CVE-2020-14196**	https://doc.powerdns.com/recursor/security-advisories/powerdns-advisory-2020-04.html, https://www.openwall.com/lists/oss-security/2020/07/01/1	A-POW-RECU-100820/730
praqma					
compatibility_action_storage					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/2/2020	4.3	Jenkins Compatibility Action Storage Plugin 1.0 and earlier does not escape the content coming from the MongoDB in the testConnection form validation endpoint, resulting in a reflected cross-site scripting (XSS) vulnerability. **CVE ID : CVE-2020-2217**	https://jenkins.io/security/advisory/2020-07-02/#SECURITY-1771	A-PRA-COMP-100820/731
Prestashop					
prestashop					
Improper Authentication	7/2/2020	10	In PrestaShop from version 1.5.0.0 and before version 1.7.6.6, the authentication system is malformed and an attacker is able to forge requests and execute admin commands. The problem is	https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-ccvh-jh5x-mpg4	A-PRE-PRES-100820/732

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			fixed in 1.7.6.6. **CVE ID : CVE-2020-4074**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/2/2020	3.5	In PrestaShop from version 1.5.3.0 and before version 1.7.6.6, there is a stored XSS when using the name of a quick access item. The problem is fixed in 1.7.6.6. **CVE ID : CVE-2020-11074**	https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-v4pg-q2cv-f7x4	A-PRE-PRES-100820/733
Improper Authentication	7/2/2020	5.5	In PrestaShop from version 1.5.0.0 and before version 1.7.6.6, there is improper access control in Carrier page, Module Manager and Module Positions. The problem is fixed in version 1.7.6.6 **CVE ID : CVE-2020-15079**	https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-xp3x-3h8q-c386	A-PRE-PRES-100820/734
Information Exposure	7/2/2020	5	In PrestaShop from version 1.7.4.0 and before version 1.7.6.6, some files should not be in the release archive, and others should not be accessible. The problem is fixed in version 1.7.6.6 A possible workaround is to make sure `composer.json` and `docker-compose.yml` are not accessible on your server. **CVE ID : CVE-2020-15080**	https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-492w-2pp5-xhvg	A-PRE-PRES-100820/735
Information Exposure	7/2/2020	5	In PrestaShop from version 1.5.0.0 and before 1.7.6.6, there is information exposure in the upload directory. The problem is fixed in version	https://github.com/PrestaShop/PrestaShop/security/advisories/GHS	A-PRE-PRES-100820/736

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.7.6.6. A possible workaround is to add an empty index.php file in the upload directory. **CVE ID : CVE-2020-15081**	A-997j-f42g-x57c	
N/A	7/2/2020	7.5	In PrestaShop from version 1.6.0.1 and before version 1.7.6.6, the dashboard allows rewriting all configuration variables. The problem is fixed in 1.7.6.6 **CVE ID : CVE-2020-15082**	https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-mc98-xjm3-c4fm	A-PRE-PRES-100820/737
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/2/2020	4.3	In PrestaShop from version 1.7.0.0 and before version 1.7.6.6, if a target sends a corrupted file, it leads to a reflected XSS. The problem is fixed in 1.7.6.6 **CVE ID : CVE-2020-15083**	https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-qgh4-95j7-p3vj	A-PRE-PRES-100820/738
protocol					
gossipsub					
N/A	7/7/2020	7.5	Gossipsub 1.0 does not properly resist invalid message spam, such as an eclipse attack or a sybil attack. **CVE ID : CVE-2020-12821**	https://gateway.ipfs.io/ipfs/QmPWuNBs8h6a8KamRvGqhTq5UDYJRQsEEy37zDKjujQQQm/Gossipsub%20Evaluation%20Report.pdf, https://github.com/ipfs/blog/pull/	A-PRO-GOSS-100820/739

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				450	
Python					
python					
Uncontrolled Search Path Element	7/4/2020	6.9	In Python 3.6 through 3.6.10, 3.7 through 3.7.8, 3.8 through 3.8.4rc1, and 3.9 through 3.9.0b4 on Windows, a Trojan horse python3.dll might be used in cases where CPython is embedded in a native application. This occurs because python3X.dll may use an invalid search path for python3.dll loading (after Py_SetPath has been used). NOTE: this issue CANNOT occur when using python.exe from a standard (non-embedded) Python installation on Windows. **CVE ID : CVE-2020-15523**	N/A	A-PYT-PYTH-100820/740
Qemu					
qemu					
NULL Pointer Dereference	7/2/2020	2.1	In QEMU 4.2.0, a MemoryRegionOps object may lack read/write callback methods, leading to a NULL pointer dereference. **CVE ID : CVE-2020-15469**	http://www.openwall.com/lists/oss-security/2020/07/02/1	A-QEM-QEMU-100820/741
Qnap					
helpdesk					
Use of Hard-coded Credentials	7/1/2020	6.4	This improper access control vulnerability in Helpdesk allows attackers to get control of QNAP	https://www.qnap.com/zh-tw/security	A-QNA-HELP-100820/742

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Kayako service. Attackers can access the sensitive data on QNAP Kayako server with API keys. We have replaced the API key to mitigate the vulnerability, and already fixed the issue in Helpdesk 3.0.1 and later versions. **CVE ID : CVE-2020-2500**	-advisory/qsa-20-03	
rack_project					
rack					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	7/2/2020	5	A directory traversal vulnerability exists in rack < 2.2.0 that allows an attacker perform directory traversal vulnerability in the Rack::Directory app that is bundled with Rack which could result in information disclosure. **CVE ID : CVE-2020-8161**	N/A	A-RAC-RACK-100820/743
raonwiz					
raon_k_upload					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	7/10/2020	7.5	RAONWIZ v2018.0.2.50 and eariler versions contains a vulnerability that could allow remote files to be downloaded and excuted by lack of validation to file extension, witch can used as remote-code-excution attacks by hackers File download & execution vulnerability in ___COMPONENT___ of RAONWIZ RAON KUpload allows ___ATTACKER/ATTACK___	N/A	A-RAO-RAON-100820/744

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			_ to cause ___IMPACT___. This issue affects: RAONWIZ RAON KUpload 2018.0.2.50 versions prior to 2018.0.2.51 on Windows. **CVE ID : CVE-2020-7814**		
red-gate					
sql_monitor					
Information Exposure	7/9/2020	4.3	In Redgate SQL Monitor 7.1.4 through 10.1.6 (inclusive), the scope for disabling some TLS security certificate checks can extend beyond that defined by various options on the Configuration > Notifications pages to disable certificate checking for alert notifications. These TLS security checks are also ignored during monitoring of VMware machines. This would make SQL Monitor vulnerable to potential man-in-the-middle attacks when sending alert notification emails, posting to Slack or posting to webhooks. The vulnerability is fixed in version 10.1.7. **CVE ID : CVE-2020-15526**	https://www.red-gate.com/privacy-and-security/vulnerabilities/2020-07-08-sql-monitor	A-RED-SQL_-100820/745
Redhat					
storage					
NULL Pointer Dereference	7/7/2020	4	A NULL pointer dereference, or possible use-after-free flaw was	N/A	A-RED-STOR-100820/746

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			found in Samba AD LDAP server in versions before 4.10.17, before 4.11.11 and before 4.12.4. Although some versions of Samba shipped with Red Hat Enterprise Linux do not support Samba in AD mode, the affected code is shipped with the libldb package. This flaw allows an authenticated user to possibly trigger a use-after-free or NULL pointer dereference. The highest threat from this vulnerability is to system availability. **CVE ID : CVE-2020-10730**		
openshift_container_platform					
Improper Check for Dropped Privileges	7/13/2020	4.6	The version of docker as released for Red Hat Enterprise Linux 7 Extras via RHBA-2020:0053 advisory included an incorrect version of runc missing the fix for CVE-2019-5736, which was previously fixed via RHSA-2019:0304. This issue could allow a malicious or compromised container to compromise the container host and other containers running on the same host. This issue only affects docker version 1.13.1-108.git4ef4b30.el7, shipped in Red Hat Enterprise Linux 7 Extras.	https://access.redhat.com/errata/RHBA-2020:0427, https://access.redhat.com/security/cve/CVE-2020-14298, https://access.redhat.com/security/vulnerabilities/runcescape, https://bugzilla.redhat.com/show_	A-RED-OPEN-100820/747

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Both earlier and later versions are not affected. **CVE ID : CVE-2020-14298**	bug.cgi?id=CVE-2019-5736	
openstack					
Out-of-bounds Read	7/9/2020	2.1	An out-of-bounds read vulnerability was found in the SLiRP networking implementation of the QEMU emulator. This flaw occurs in the icmp6_send_echoreply() routine while replying to an ICMP echo request, also known as ping. This flaw allows a malicious guest to leak the contents of the host memory, resulting in possible information disclosure. This flaw affects versions of libslirp before 4.3.1. **CVE ID : CVE-2020-10756**	N/A	A-RED-OPEN-100820/748
rittal					
iot_interface_3124.300					
Use of Hard-coded Credentials	7/14/2020	10	An issue was discovered on Rittal PDU-3C002DEC through 5.17.10 and CMCIII-PU-9333E0FB through 3.17.10 devices. There is a Backdoor root account. **CVE ID : CVE-2020-11951**	N/A	A-RIT-IOT_-100820/749
Information Exposure	7/14/2020	4.9	An issue was discovered on Rittal PDU-3C002DEC through 5.17.10 and CMCIII-PU-9333E0FB through 3.17.10 devices. Attackers can bypass the	N/A	A-RIT-IOT_-100820/750

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CLI menu. **CVE ID : CVE-2020-11952**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	7/14/2020	9	An issue was discovered on Rittal PDU-3C002DEC through 5.15.40 and CMCIII-PU-9333E0FB through 3.15.70_4 devices. Attackers can execute code. **CVE ID : CVE-2020-11953**	N/A	A-RIT-IOT_-100820/751
Incorrect Default Permissions	7/14/2020	9	An issue was discovered on Rittal PDU-3C002DEC through 5.15.70 and CMCIII-PU-9333E0FB through 3.15.70 devices. There are insecure permissions. **CVE ID : CVE-2020-11955**	N/A	A-RIT-IOT_-100820/752
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	7/14/2020	10	An issue was discovered on Rittal PDU-3C002DEC through 5.17.10 and CMCIII-PU-9333E0FB through 3.17.10 devices. There is a least privilege violation. **CVE ID : CVE-2020-11956**	N/A	A-RIT-IOT_-100820/753
Rockwellautomation					
logix_designer_studio_5000					
Improper Restriction of XML External Entity Reference ('XXE')	7/14/2020	4.3	Rockwell Automation Logix Designer Studio 5000 Versions 32.00, 32.01, and 32.02 vulnerable to an xml external entity (XXE) vulnerability, which may allow an attacker to view hostnames or other resources from the	N/A	A-ROC-LOGI-100820/754

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			program. **CVE ID : CVE-2020-12025**		
rosariosis					
rosariosis					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/15/2020	4.3	RosarioSIS 6.7.2 is vulnerable to XSS, caused by improper validation of user-supplied input by the Preferences.php script. A remote attacker could exploit this vulnerability using the tab parameter in a crafted URL. **CVE ID : CVE-2020-15716**	https://gitlab.com/francoisjacquet/rosariosis/-/commit/89ae9de732024e3a2e99262aa98b400a1aa6975a	A-ROS-ROSA-100820/755
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/15/2020	4.3	RosarioSIS 6.7.2 is vulnerable to XSS, caused by improper validation of user-supplied input by the Search.inc.php script. A remote attacker could exploit this vulnerability using the advanced parameter in a crafted URL. **CVE ID : CVE-2020-15717**	https://gitlab.com/francoisjacquet/rosariosis/-/commit/89ae9de732024e3a2e99262aa98b400a1aa6975a	A-ROS-ROSA-100820/756
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/15/2020	4.3	RosarioSIS 6.7.2 is vulnerable to XSS, caused by improper validation of user-supplied input by the PrintSchedules.php script. A remote attacker could exploit this vulnerability using the include_inactive parameter in a crafted URL. **CVE ID : CVE-2020-15718**	https://gitlab.com/francoisjacquet/rosariosis/-/commit/89ae9de732024e3a2e99262aa98b400a1aa6975a	A-ROS-ROSA-100820/757
Improper	7/14/2020	4.3	RosarioSIS through 6.8-	N/A	A-ROS-ROSA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			beta allows modules/Custom/NotifyParents.php XSS because of the href attributes for AddStudents.php and User.php. **CVE ID : CVE-2020-15721**		100820/758
Roundcube					
webmail					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/6/2020	4.3	An issue was discovered in Roundcube Webmail before 1.2.11, 1.3.x before 1.3.14, and 1.4.x before 1.4.7. It allows XSS via a crafted HTML e-mail message, as demonstrated by a JavaScript payload in the xmlns (aka XML namespace) attribute of a HEAD element when an SVG element exists. **CVE ID : CVE-2020-15562**	N/A	A-ROU-WEBM-100820/759
Rubyonrails					
rails					
Improper Control of Generation of Code ('Code Injection')	7/2/2020	6.5	The is a code injection vulnerability in versions of Rails prior to 5.0.1 that wouldallow an attacker who controlled the \`locals\` argument of a \`render\` call to perform a RCE. **CVE ID : CVE-2020-8163**	N/A	A-RUB-RAIL-100820/760
Cross-Site Request Forgery (CSRF)	7/2/2020	4.3	A CSRF forgery vulnerability exists in rails < 5.2.5, rails < 6.0.4 that makes it possible for an attacker to, given a global CSRF token such as the one	N/A	A-RUB-RAIL-100820/761

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			present in the authenticity_token meta tag, forge a per-form CSRF token. **CVE ID : CVE-2020-8166**		
Uncontrolled Resource Consumption	7/2/2020	4	A denial of service vulnerability exists in Rails <6.0.3.2 that allowed an untrusted user to run any pending migrations on a Rails app running in production. **CVE ID : CVE-2020-8185**	N/A	A-RUB-RAIL-100820/762
Samba					
samba					
NULL Pointer Dereference	7/7/2020	4	A NULL pointer dereference, or possible use-after-free flaw was found in Samba AD LDAP server in versions before 4.10.17, before 4.11.11 and before 4.12.4. Although some versions of Samba shipped with Red Hat Enterprise Linux do not support Samba in AD mode, the affected code is shipped with the libldb package. This flaw allows an authenticated user to possibly trigger a use-after-free or NULL pointer dereference. The highest threat from this vulnerability is to system availability. **CVE ID : CVE-2020-10730**	N/A	A-SAM-SAMB-100820/763
Uncontrolled Resource	7/7/2020	7.8	A flaw was found in all Samba versions before	N/A	A-SAM-SAMB-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Consumption			4.10.17, before 4.11.11 and before 4.12.4 in the way it processed NetBios over TCP/IP. This flaw allows a remote attacker could to cause the Samba server to consume excessive CPU use, resulting in a denial of service. This highest threat from this vulnerability is to system availability. **CVE ID : CVE-2020-10745**		100820/764
Use After Free	7/6/2020	4	A use-after-free flaw was found in all samba LDAP server versions before 4.10.17, before 4.11.11, before 4.12.4 used in a AC DC configuration. A Samba LDAP user could use this flaw to crash samba. **CVE ID : CVE-2020-10760**	N/A	A-SAM-SAMB-100820/765
Improper Input Validation	7/6/2020	5	A flaw was found in the AD DC NBT server in all Samba versions before 4.10.17, before 4.11.11 and before 4.12.4. A samba user could send an empty UDP packet to cause the samba server to crash. **CVE ID : CVE-2020-14303**	https://security.netapp.com/advisory/ntap-20200709-0003/	A-SAM-SAMB-100820/766
SAP					
abap_platform					
Information Exposure	7/14/2020	4	SAP NetWeaver (ABAP Server) and ABAP Platform, versions 731, 740, 750, allows an attacker with admin privileges to access certain files which should	N/A	A-SAP-ABAP-100820/767

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			otherwise be restricted, leading to Information Disclosure. **CVE ID : CVE-2020-6280**		
solution_manager					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	7/1/2020	5	SAP Solution Manager (Trace Analysis), version 7.20, allows an attacker to perform a log injection into the trace file, due to Incomplete XML Validation. The readability of the trace file is impaired. **CVE ID : CVE-2020-6261**	N/A	A-SAP-SOLU-100820/768
netweaver					
Information Exposure	7/14/2020	3.5	SAP NetWeaver - XML Toolkit for JAVA (ENGINEAPI) (versions- 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50), under certain conditions allows an attacker to access information which would otherwise be restricted, leading to Information Disclosure. **CVE ID : CVE-2020-6285**	N/A	A-SAP-NETW-100820/769
disclosure_management					
Incorrect Permission Assignment for Critical Resource	7/14/2020	5.8	Some sensitive cookies in SAP Disclosure Management, version 10.1, are missing HttpOnly flag, leading to sensitive cookie without Http Only flag. **CVE ID : CVE-2020-6267**	N/A	A-SAP-DISC-100820/770
Cross-Site Request	7/14/2020	6.8	SAP Disclosure Management, version 10.1, had insufficient protection	N/A	A-SAP-DISC-100820/771

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			against Cross-Site Request Forgery, which could be used to trick user in to browsing malicious site. **CVE ID : CVE-2020-6289**		
Session Fixation	7/14/2020	6.8	SAP Disclosure Management, version 10.1, is vulnerable to Session Fixation attacks wherein the attacker tricks the user into using a specific session ID. **CVE ID : CVE-2020-6290**	N/A	A-SAP-DISC-100820/772
Insufficient Session Expiration	7/14/2020	6.5	SAP Disclosure Management, version 10.1, session mechanism does not have expiration data set therefore allows unlimited access after authenticating once, leading to Insufficient Session Expiration **CVE ID : CVE-2020-6291**	N/A	A-SAP-DISC-100820/773
Insufficient Session Expiration	7/14/2020	6.5	Logout mechanism in SAP Disclosure Management, version 10.1, does not invalidate one of the session cookies, leading to Insufficient Session Expiration. **CVE ID : CVE-2020-6292**	N/A	A-SAP-DISC-100820/774
netweaver_application_server_java					
Server-Side Request Forgery (SSRF)	7/14/2020	5	SAP NetWeaver AS JAVA (IIOP service) (SERVERCORE), versions 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, and SAP NetWeaver AS JAVA (IIOP	N/A	A-SAP-NETW-100820/775

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service) (CORE-TOOLS), versions 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, allows an attacker to send a crafted request from a vulnerable web application. It is usually used to target internal systems behind firewalls that are normally inaccessible to an attacker from the external network, resulting in a Server-Side Request Forgery vulnerability. **CVE ID : CVE-2020-6282**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	7/14/2020	5	The insufficient input path validation of certain parameter in the web service of SAP NetWeaver AS JAVA (LM Configuration Wizard), versions - 7.30, 7.31, 7.40, 7.50, allows an unauthenticated attacker to exploit a method to download zip files to a specific directory, leading to Path Traversal. **CVE ID : CVE-2020-6286**	N/A	A-SAP-NETW-100820/776
Improper Authentication	7/14/2020	10	SAP NetWeaver AS JAVA (LM Configuration Wizard), versions - 7.30, 7.31, 7.40, 7.50, does not perform an authentication check which allows an attacker without prior authentication to execute configuration tasks to perform critical actions against the SAP Java	N/A	A-SAP-NETW-100820/777

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system, including the ability to create an administrative user, and therefore compromising Confidentiality, Integrity and Availability of the system, leading to Missing Authentication Check. **CVE ID : CVE-2020-6287**		
netweaver_as_abap					
Information Exposure	7/14/2020	4	SAP NetWeaver (ABAP Server) and ABAP Platform, versions 731, 740, 750, allows an attacker with admin privileges to access certain files which should otherwise be restricted, leading to Information Disclosure. **CVE ID : CVE-2020-6280**	N/A	A-SAP-NETW-100820/778
businessobjects_business_intelligence_platform					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/14/2020	4.3	SAP Business Objects Business Intelligence Platform (bipodata), version 4.2, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting vulnerability. **CVE ID : CVE-2020-6276**	N/A	A-SAP-BUSI-100820/779
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/14/2020	3.5	SAP Business Objects Business Intelligence Platform (BI Launchpad and CMC), versions 4.1, 4.2, allows to an attacker to embed malicious scripts in the application while uploading images, which	N/A	A-SAP-BUSI-100820/780

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			gets executed when the victim opens these files, leading to Stored Cross Site Scripting **CVE ID : CVE-2020-6278**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/14/2020	4.3	SAP Business Objects Business Intelligence Platform (BI Launchpad), version 4.2, does not sufficiently encode user-controlled inputs, resulting reflected in Cross-Site Scripting. **CVE ID : CVE-2020-6281**	N/A	A-SAP-BUSI-100820/781
schokokeks					
freewvs					
Uncontrolled Resource Consumption	7/14/2020	2.1	In freewvs before 0.1.1, a user could create a large file that freewvs will try to read, which will terminate a scan process. This has been patched in 0.1.1. **CVE ID : CVE-2020-15100**	https://github.com/schokokeksorg/freewvs/security/advisories/GHSA-9cfv-9463-8gqv	A-SCH-FREE-100820/782
Uncontrolled Resource Consumption	7/14/2020	4	In freewvs before 0.1.1, a directory structure of more than 1000 nested directories can interrupt a freewvs scan due to Python's recursion limit and os.walk(). This can be problematic in a case where an administrator scans the dirs of potentially untrusted users. This has been patched in 0.1.1. **CVE ID : CVE-2020-15101**	https://github.com/schokokeksorg/freewvs/security/advisories/GHSA-7pmh-vrww-25xx	A-SCH-FREE-100820/783

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
seczetta					
neprofile					
Unrestricted Upload of File with Dangerous Type	7/15/2020	6.5	A remote code execution vulnerability was identified in SecZetta NEProfile 3.3.11. Authenticated remote adversaries can invoke code execution upon uploading a carefully crafted JPEG file as part of the profile avatar. **CVE ID : CVE-2020-12854**	N/A	A-SEC-NEPR-100820/784
shopify					
koa-shopify-auth					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/2/2020	4.3	A cross-site scripting vulnerability exists in koa-shopify-auth v3.1.61-v3.1.62 that allows an attacker to inject JS payloads into the \`shop\` parameter on the \`/shopify/auth/enable_cookies\` endpoint. **CVE ID : CVE-2020-8176**	N/A	A-SHO-KOA--100820/785
Siemens					
simatic_wincc_runtime_advanced					
Cleartext Transmission of Sensitive Information	7/14/2020	3.3	A vulnerability has been identified in SIMATIC HMI Basic Panels 1st Generation (incl. SIPLUS variants) (All versions), SIMATIC HMI Basic Panels 2nd Generation (incl. SIPLUS variants) (All versions), SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All	N/A	A-SIE-SIMA-100820/786

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC HMI KTP700F Mobile Arctic (All versions), SIMATIC HMI Mobile Panels 2nd Generation (All versions), SIMATIC WinCC Runtime Advanced (All versions). Unencrypted communication between the configuration software and the respective device could allow an attacker to capture potential plain text communication and have access to sensitive information. **CVE ID : CVE-2020-7592**		
simatic_pcs_neo					
Unquoted Search Path or Element	7/14/2020	7.2	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft	N/A	A-SIE-SIMA-100820/787

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Starter ES (All versions). A component within the affected application calls a helper binary with SYSTEM privileges during startup while the call path is not quoted. **CVE ID : CVE-2020-7581**		
Uncontrolled Resource Consumption	7/14/2020	6.4	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC IT LMS (All versions), SIMATIC IT Production Suite (All versions), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES (All versions). Sending multiple specially crafted packets to the affected service could cause a partial remote Denial-of-Service, that would cause the service to restart itself.	N/A	A-SIE-SIMA-100820/788

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			On some cases the vulnerability could leak random information from the remote service. **CVE ID : CVE-2020-7587**		
Improper Input Validation	7/14/2020	5	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC IT LMS (All versions), SIMATIC IT Production Suite (All versions), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES (All versions). Sending a specially crafted packet to the affected service could cause a partial remote Denial-of-Service, that would cause the service to restart itself. **CVE ID : CVE-2020-7588**	N/A	A-SIE-SIMA-100820/789
simatic_step_7					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unquoted Search Path or Element	7/14/2020	7.2	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES (All versions). A component within the affected application calls a helper binary with SYSTEM privileges during startup while the call path is not quoted. **CVE ID : CVE-2020-7581**	N/A	A-SIE-SIMA-100820/790
Uncontrolled Resource Consumption	7/14/2020	6.4	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3),	N/A	A-SIE-SIMA-100820/791

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Opcenter RD&L (V8.0), SIMATIC IT LMS (All versions), SIMATIC IT Production Suite (All versions), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES (All versions). Sending multiple specially crafted packets to the affected service could cause a partial remote Denial-of-Service, that would cause the service to restart itself. On some cases the vulnerability could leak random information from the remote service. **CVE ID : CVE-2020-7587**		
Improper Input Validation	7/14/2020	5	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC IT LMS (All versions), SIMATIC IT	N/A	A-SIE-SIMA-100820/792

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Production Suite (All versions), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES (All versions). Sending a specially crafted packet to the affected service could cause a partial remote Denial-of-Service, that would cause the service to restart itself. **CVE ID : CVE-2020-7588**		
opcenter_execution_discrete					
Unquoted Search Path or Element	7/14/2020	7.2	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA	N/A	A-SIE-OPCE-100820/793

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES (All versions). A component within the affected application calls a helper binary with SYSTEM privileges during startup while the call path is not quoted. **CVE ID : CVE-2020-7581**		
Uncontrolled Resource Consumption	7/14/2020	6.4	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC IT LMS (All versions), SIMATIC IT Production Suite (All versions), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES (All versions). Sending multiple specially crafted packets to the affected service could cause a	N/A	A-SIE-OPCE-100820/794

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			partial remote Denial-of-Service, that would cause the service to restart itself. On some cases the vulnerability could leak random information from the remote service. **CVE ID : CVE-2020-7587**		
Improper Input Validation	7/14/2020	5	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC IT LMS (All versions), SIMATIC IT Production Suite (All versions), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES (All versions). Sending a specially crafted packet to the affected service could cause a partial remote Denial-of-Service, that would cause the service to	N/A	A-SIE-OPCE-100820/795

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			restart itself. **CVE ID : CVE-2020-7588**		
opcenter_execution_foundation					
Unquoted Search Path or Element	7/14/2020	7.2	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES (All versions). A component within the affected application calls a helper binary with SYSTEM privileges during startup while the call path is not quoted. **CVE ID : CVE-2020-7581**	N/A	A-SIE-OPCE-100820/796
Uncontrolled Resource Consumption	7/14/2020	6.4	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All	N/A	A-SIE-OPCE-100820/797

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC IT LMS (All versions), SIMATIC IT Production Suite (All versions), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES (All versions). Sending multiple specially crafted packets to the affected service could cause a partial remote Denial-of-Service, that would cause the service to restart itself. On some cases the vulnerability could leak random information from the remote service. **CVE ID : CVE-2020-7587**		
Improper Input Validation	7/14/2020	5	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All	N/A	A-SIE-OPCE-100820/798

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions < V11.3), Opcenter RD&L (V8.0), SIMATIC IT LMS (All versions), SIMATIC IT Production Suite (All versions), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES (All versions). Sending a specially crafted packet to the affected service could cause a partial remote Denial-of-Service, that would cause the service to restart itself. **CVE ID : CVE-2020-7588**		
opcenter_execution_process					
Unquoted Search Path or Element	7/14/2020	7.2	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS	N/A	A-SIE-OPCE-100820/799

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES (All versions). A component within the affected application calls a helper binary with SYSTEM privileges during startup while the call path is not quoted. **CVE ID : CVE-2020-7581**		
Uncontrolled Resource Consumption	7/14/2020	6.4	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC IT LMS (All versions), SIMATIC IT Production Suite (All versions), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES	N/A	A-SIE-OPCE-100820/800

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions). Sending multiple specially crafted packets to the affected service could cause a partial remote Denial-of-Service, that would cause the service to restart itself. On some cases the vulnerability could leak random information from the remote service. **CVE ID : CVE-2020-7587**		
Improper Input Validation	7/14/2020	5	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC IT LMS (All versions), SIMATIC IT Production Suite (All versions), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES (All versions). Sending a specially crafted packet to the affected service could	N/A	A-SIE-OPCE-100820/801

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cause a partial remote Denial-of-Service, that would cause the service to restart itself. **CVE ID : CVE-2020-7588**		
opcenter_intelligence					
Unquoted Search Path or Element	7/14/2020	7.2	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES (All versions). A component within the affected application calls a helper binary with SYSTEM privileges during startup while the call path is not quoted. **CVE ID : CVE-2020-7581**	N/A	A-SIE-OPCE-100820/802
Uncontrolled Resource Consumption	7/14/2020	6.4	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter	N/A	A-SIE-OPCE-100820/803

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC IT LMS (All versions), SIMATIC IT Production Suite (All versions), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES (All versions). Sending multiple specially crafted packets to the affected service could cause a partial remote Denial-of-Service, that would cause the service to restart itself. On some cases the vulnerability could leak random information from the remote service. **CVE ID : CVE-2020-7587**		
Improper Input Validation	7/14/2020	5	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All	N/A	A-SIE-OPCE-100820/804

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC IT LMS (All versions), SIMATIC IT Production Suite (All versions), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES (All versions). Sending a specially crafted packet to the affected service could cause a partial remote Denial-of-Service, that would cause the service to restart itself. **CVE ID : CVE-2020-7588**		
opcenter_quality					
Unquoted Search Path or Element	7/14/2020	7.2	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0),	N/A	A-SIE-OPCE-100820/805

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES (All versions). A component within the affected application calls a helper binary with SYSTEM privileges during startup while the call path is not quoted. **CVE ID : CVE-2020-7581**		
Uncontrolled Resource Consumption	7/14/2020	6.4	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC IT LMS (All versions), SIMATIC IT Production Suite (All versions), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All	N/A	A-SIE-OPCE-100820/806

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES (All versions). Sending multiple specially crafted packets to the affected service could cause a partial remote Denial-of-Service, that would cause the service to restart itself. On some cases the vulnerability could leak random information from the remote service. **CVE ID : CVE-2020-7587**		
Improper Input Validation	7/14/2020	5	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC IT LMS (All versions), SIMATIC IT Production Suite (All versions), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES	N/A	A-SIE-OPCE-100820/807

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions). Sending a specially crafted packet to the affected service could cause a partial remote Denial-of-Service, that would cause the service to restart itself. **CVE ID : CVE-2020-7588**		
opcenter_rd\&l					
Unquoted Search Path or Element	7/14/2020	7.2	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES (All versions). A component within the affected application calls a helper binary with SYSTEM privileges during startup while the call path is not quoted. **CVE ID : CVE-2020-7581**	N/A	A-SIE-OPCE-100820/808

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	7/14/2020	6.4	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC IT LMS (All versions), SIMATIC IT Production Suite (All versions), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES (All versions). Sending multiple specially crafted packets to the affected service could cause a partial remote Denial-of-Service, that would cause the service to restart itself. On some cases the vulnerability could leak random information from the remote service. **CVE ID : CVE-2020-7587**	N/A	A-SIE-OPCE-100820/809
Improper Input Validation	7/14/2020	5	A vulnerability has been identified in Opcenter Execution Discrete (All	N/A	A-SIE-OPCE-100820/810

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC IT LMS (All versions), SIMATIC IT Production Suite (All versions), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES (All versions). Sending a specially crafted packet to the affected service could cause a partial remote Denial-of-Service, that would cause the service to restart itself. **CVE ID : CVE-2020-7588**		
simatic_notifier_server					
Unquoted Search Path or Element	7/14/2020	7.2	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter	N/A	A-SIE-SIMA-100820/811

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES (All versions). A component within the affected application calls a helper binary with SYSTEM privileges during startup while the call path is not quoted. **CVE ID : CVE-2020-7581**		
Uncontrolled Resource Consumption	7/14/2020	6.4	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC IT LMS (All versions), SIMATIC IT Production Suite (All versions), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All	N/A	A-SIE-SIMA-100820/812

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES (All versions). Sending multiple specially crafted packets to the affected service could cause a partial remote Denial-of-Service, that would cause the service to restart itself. On some cases the vulnerability could leak random information from the remote service. **CVE ID : CVE-2020-7587**		
Improper Input Validation	7/14/2020	5	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC IT LMS (All versions), SIMATIC IT Production Suite (All versions), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7	N/A	A-SIE-SIMA-100820/813

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES (All versions). Sending a specially crafted packet to the affected service could cause a partial remote Denial-of-Service, that would cause the service to restart itself. **CVE ID : CVE-2020-7588**		
simocode_es					
Unquoted Search Path or Element	7/14/2020	7.2	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES (All versions). A component within the affected application calls a helper binary with SYSTEM privileges during	N/A	A-SIE-SIMO-100820/814

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			startup while the call path is not quoted. **CVE ID : CVE-2020-7581**		
Uncontrolled Resource Consumption	7/14/2020	6.4	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC IT LMS (All versions), SIMATIC IT Production Suite (All versions), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES (All versions). Sending multiple specially crafted packets to the affected service could cause a partial remote Denial-of-Service, that would cause the service to restart itself. On some cases the vulnerability could leak random information from the remote service.	N/A	A-SIE-SIMO-100820/815

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7587		
Improper Input Validation	7/14/2020	5	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC IT LMS (All versions), SIMATIC IT Production Suite (All versions), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES (All versions). Sending a specially crafted packet to the affected service could cause a partial remote Denial-of-Service, that would cause the service to restart itself. **CVE ID : CVE-2020-7588**	N/A	A-SIE-SIMO-100820/816
soft_starter_es					
Unquoted Search Path or Element	7/14/2020	7.2	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter	N/A	A-SIE-SOFT-100820/817

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES (All versions). A component within the affected application calls a helper binary with SYSTEM privileges during startup while the call path is not quoted. **CVE ID : CVE-2020-7581**		
Uncontrolled Resource Consumption	7/14/2020	6.4	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC IT LMS (All versions), SIMATIC IT Production Suite (All	N/A	A-SIE-SOFT-100820/818

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES (All versions). Sending multiple specially crafted packets to the affected service could cause a partial remote Denial-of-Service, that would cause the service to restart itself. On some cases the vulnerability could leak random information from the remote service. **CVE ID : CVE-2020-7587**		
Improper Input Validation	7/14/2020	5	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC IT LMS (All versions), SIMATIC IT Production Suite (All versions), SIMATIC Notifier Server for Windows (All versions),	N/A	A-SIE-SOFT-100820/819

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES (All versions). Sending a specially crafted packet to the affected service could cause a partial remote Denial-of-Service, that would cause the service to restart itself. **CVE ID : CVE-2020-7588**		
simatic_it_lms					
Uncontrolled Resource Consumption	7/14/2020	6.4	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC IT LMS (All versions), SIMATIC IT Production Suite (All versions), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All	N/A	A-SIE-SIMA-100820/820

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES (All versions). Sending multiple specially crafted packets to the affected service could cause a partial remote Denial-of-Service, that would cause the service to restart itself. On some cases the vulnerability could leak random information from the remote service. **CVE ID : CVE-2020-7587**		
Improper Input Validation	7/14/2020	5	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC IT LMS (All versions), SIMATIC IT Production Suite (All versions), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES	N/A	A-SIE-SIMA-100820/821

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions). Sending a specially crafted packet to the affected service could cause a partial remote Denial-of-Service, that would cause the service to restart itself. **CVE ID : CVE-2020-7588**		
simatic_it_production_suite					
Uncontrolled Resource Consumption	7/14/2020	6.4	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC IT LMS (All versions), SIMATIC IT Production Suite (All versions), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES (All versions). Sending multiple specially crafted packets to the affected service could cause a partial remote Denial-of-	N/A	A-SIE-SIMA-100820/822

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service, that would cause the service to restart itself. On some cases the vulnerability could leak random information from the remote service. **CVE ID : CVE-2020-7587**		
Improper Input Validation	7/14/2020	5	A vulnerability has been identified in Opcenter Execution Discrete (All versions < V3.2), Opcenter Execution Foundation (All versions < V3.2), Opcenter Execution Process (All versions < V3.2), Opcenter Intelligence (All versions), Opcenter Quality (All versions < V11.3), Opcenter RD&L (V8.0), SIMATIC IT LMS (All versions), SIMATIC IT Production Suite (All versions), SIMATIC Notifier Server for Windows (All versions), SIMATIC PCS neo (All versions), SIMATIC STEP 7 (TIA Portal) V15 (All versions), SIMATIC STEP 7 (TIA Portal) V16 (All versions < V16 Update 2), SIMOCODE ES (All versions), Soft Starter ES (All versions). Sending a specially crafted packet to the affected service could cause a partial remote Denial-of-Service, that would cause the service to restart itself.	N/A	A-SIE-SIMA-100820/823

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7588		
simatic_hmi_basic_panels_1st_generation					
Cleartext Transmission of Sensitive Information	7/14/2020	3.3	A vulnerability has been identified in SIMATIC HMI Basic Panels 1st Generation (incl. SIPLUS variants) (All versions), SIMATIC HMI Basic Panels 2nd Generation (incl. SIPLUS variants) (All versions), SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions), SIMATIC HMI KTP700F Mobile Arctic (All versions), SIMATIC HMI Mobile Panels 2nd Generation (All versions), SIMATIC WinCC Runtime Advanced (All versions). Unencrypted communication between the configuration software and the respective device could allow an attacker to capture potential plain text communication and have access to sensitive information. **CVE ID : CVE-2020-7592**	N/A	A-SIE-SIMA-100820/824
simatic_hmi_basic_panels_2nd_generation					
Cleartext Transmission of Sensitive Information	7/14/2020	3.3	A vulnerability has been identified in SIMATIC HMI Basic Panels 1st Generation (incl. SIPLUS variants) (All versions), SIMATIC HMI Basic Panels 2nd Generation (incl. SIPLUS variants) (All versions), SIMATIC HMI	N/A	A-SIE-SIMA-100820/825

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Comfort Panels (incl. SIPLUS variants) (All versions), SIMATIC HMI KTP700F Mobile Arctic (All versions), SIMATIC HMI Mobile Panels 2nd Generation (All versions), SIMATIC WinCC Runtime Advanced (All versions). Unencrypted communication between the configuration software and the respective device could allow an attacker to capture potential plain text communication and have access to sensitive information. **CVE ID : CVE-2020-7592**		
opcenter_execution_core					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/14/2020	3.5	A vulnerability has been identified in Camstar Enterprise Platform (All versions), Opcenter Execution Core (All versions < V8.2). An authenticated user with the ability to create containers, packages or register defects could perform stored Cross-Site Scripting (XSS) attacks within the vulnerable software. The impact of this attack could result in the session cookies of legitimate users being stolen. Should the attacker gain access to these cookies, they could then	N/A	A-SIE-OPCE-100820/826

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			hijack the session and perform arbitrary actions in the name of the victim. **CVE ID : CVE-2020-7576**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	7/14/2020	5.5	A vulnerability has been identified in Camstar Enterprise Platform (All versions), Opcenter Execution Core (All versions < V8.2). Through the use of several vulnerable fields of the application, an authenticated user could perform an SQL Injection attack by passing a modified SQL query downstream to the back-end server. The exploit of this vulnerability could be used to read, and potentially modify application data to which the user has access to. **CVE ID : CVE-2020-7577**	N/A	A-SIE-OPCE-100820/827
Improper Privilege Management	7/14/2020	5.5	A vulnerability has been identified in Camstar Enterprise Platform (All versions), Opcenter Execution Core (All versions < V8.2). Authenticated users could have access to resources they normally would not have. This vulnerability could allow an attacker to view internal information and perform unauthorized changes.	N/A	A-SIE-OPCE-100820/828

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7578		
Silverstripe					
mimevalidator					
Unrestricted Upload of File with Dangerous Type	7/15/2020	6.8	Silverstripe CMS through 4.5 can be susceptible to script execution from malicious upload contents under allowed file extensions (for example HTML code in a TXT file). When these files are stored as protected or draft files, the MIME detection can cause browsers to execute the file contents. Uploads stored as protected or draft files are allowed by default for authorised users only, but can also be enabled through custom logic as well as modules such as silverstripe/userforms. Sites using the previously optional silverstripe/mimevalidator module can configure MIME whitelists rather than extension whitelists, and hence prevent this issue. Sites on the Common Web Platform (CWP) use this module by default, and are not affected. **CVE ID : CVE-2020-9309**	https://www.silverstripe.org/download/security-releases/CVE-2020-9309	A-SIL-MIME-100820/829
recipe					
Unrestricted Upload of File with	7/15/2020	6.8	Silverstripe CMS through 4.5 can be susceptible to script execution from	https://www.silverstripe.org/dow	A-SIL-RECI-100820/830

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			malicious upload contents under allowed file extensions (for example HTML code in a TXT file). When these files are stored as protected or draft files, the MIME detection can cause browsers to execute the file contents. Uploads stored as protected or draft files are allowed by default for authorised users only, but can also be enabled through custom logic as well as modules such as silverstripe/userforms. Sites using the previously optional silverstripe/mimevalidator module can configure MIME whitelists rather than extension whitelists, and hence prevent this issue. Sites on the Common Web Platform (CWP) use this module by default, and are not affected. **CVE ID : CVE-2020-9309**	nload/security-releases/CVE-2020-9309	
silverstripe					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/15/2020	3.5	In SilverStripe through 4.5, malicious users with a valid Silverstripe CMS login (usually CMS access) can craft profile information which can lead to XSS for other users through specially crafted login form URLs. **CVE ID : CVE-2020-9311**	https://www.silverstripe.org/download/security-releases/CVE-2020-9311	A-SIL-SILV-100820/831

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	7/15/2020	5	In SilverStripe through 4.5.0, a specific URL path configured by default through the silverstripe/framework module can be used to disclose the fact that a domain is hosting a Silverstripe application. There is no disclosure of the specific version. The functionality on this URL path is limited to execution in a CLI context, and is not known to present a vulnerability through web-based access. As a side-effect, this preconfigured path also blocks the creation of other resources on this path (e.g. a page). **CVE ID : CVE-2020-6164**	https://www.silverstripe.org/download/security-releases/CVE-2020-6164	A-SIL-SILV-100820/832
Incorrect Default Permissions	7/15/2020	5	SilverStripe 4.5.0 allows attackers to read certain records that should not have been placed into a result set. This affects silverstripe/recipe-cms. The automatic permission-checking mechanism in the silverstripe/graphql module does not provide complete protection against lists that are limited (e.g., through pagination), resulting in records that should have failed a permission check being added to the final result set. GraphQL endpoints are configured	N/A	A-SIL-SILV-100820/833

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			by default (e.g., for assets), but the admin/graphql endpoint is access protected by default. This limits the vulnerability to all authenticated users, including those with limited permissions (e.g., where viewing records exposed through admin/graphql requires administrator permissions). However, if custom GraphQL endpoints have been configured for a specific implementation (usually under /graphql), this vulnerability could also be exploited through unauthenticated requests. This vulnerability only applies to reading records; it does not allow unauthorised changing of records. **CVE ID : CVE-2020-6165**		
socket.io-file_project					
socket.io-file					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	7/15/2020	5	A Path Traversal issue was discovered in the socket.io-file package through 2.0.31 for Node.js. The socket.io-file::createFile message uses path.join with ../ in the name option, and the uploadDir and rename options determine the path. **CVE ID : CVE-2020-15779**	N/A	A-SOC-SOCK-100820/834

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sockjs_project					
sockjs					
Improper Input Validation	7/9/2020	5	Incorrect handling of Upgrade header with the value websocket leads in crashing of containers hosting sockjs apps. This affects the package sockjs before 0.3.20. **CVE ID : CVE-2020-7693**	N/A	A-SOC-SOCK-100820/835
Solarwinds					
serv-u					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/7/2020	4.3	SolarWinds Serv-U File Server before 15.2.1 has a "Cross-script vulnerability," aka Case Numbers 00041778 and 00306421. **CVE ID : CVE-2020-15573**	https://documentation.solarwinds.com/en/success_center/servu/Content/Release_Notes/Servu_15-2-1_release_notes.htm	A-SOL-SERV-100820/836
Missing Encryption of Sensitive Data	7/7/2020	5	SolarWinds Serv-U File Server before 15.2.1 mishandles the Same-Site cookie attribute, aka Case Number 00331893. **CVE ID : CVE-2020-15574**	https://documentation.solarwinds.com/en/success_center/servu/Content/Release_Notes/Servu_15-2-1_release_notes.htm	A-SOL-SERV-100820/837
Improper Neutralization of Input During Web Page Generation	7/7/2020	4.3	SolarWinds Serv-U File Server before 15.2.1 allows XSS as demonstrated by Tenable Scan, aka Case	https://documentation.solarwinds.com/en/success_center	A-SOL-SERV-100820/838

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Number 00484194. **CVE ID : CVE-2020-15575**	/servu/Content/Release_Notes/Servu_15-2-1_release_notes.htm	
Information Exposure	7/7/2020	5	SolarWinds Serv-U File Server before 15.2.1 allows information disclosure via an HTTP response. **CVE ID : CVE-2020-15576**	https://documentation.solarwinds.com/en/success_center/servu/Content/Release_Notes/Servu_15-2-1_release_notes.htm	A-SOL-SERV-100820/839
serv-u_ftp_server					
Improper Control of Generation of Code ('Code Injection')	7/5/2020	7.5	SolarWinds Serv-U FTP server before 15.2.1 allows remote command execution. **CVE ID : CVE-2020-15541**	N/A	A-SOL-SERV-100820/840
N/A	7/5/2020	7.5	SolarWinds Serv-U FTP server before 15.2.1 mishandles the CHMOD command. **CVE ID : CVE-2020-15542**	N/A	A-SOL-SERV-100820/841
Improper Input Validation	7/5/2020	7.5	SolarWinds Serv-U FTP server before 15.2.1 does not validate an argument path. **CVE ID : CVE-2020-15543**	N/A	A-SOL-SERV-100820/842
srs_simple_hits_counter_project					
srs_simple_hits_counter					
Improper Neutralization of Special	7/13/2020	5	Improper Neutralization of Special Elements used in an SQL Command ('SQL	https://www.tenable.com/securit	A-SRS-SRS_-100820/843

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			Injection') in SRS Simple Hits Counter Plugin for WordPress 1.0.3 and 1.0.4 allows a remote, unauthenticated attacker to determine the value of database fields. **CVE ID : CVE-2020-5766**	y/research/tra-2020-42	
ss-proj					
shirasagi					
URL Redirection to Untrusted Site ('Open Redirect')	7/10/2020	5.8	Open redirect vulnerability in SHIRASAGI v1.13.1 and earlier allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors. **CVE ID : CVE-2020-5607**	N/A	A-SS--SHIR-100820/844
Superwebmailer					
superwebmailer					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	7/14/2020	7.5	SuperWebMailer 7.21.0.01526 is susceptible to a remote code execution vulnerability in the Language parameter of mailingupgrade.php. An unauthenticated remote attacker can exploit this behavior to execute arbitrary PHP code via Code Injection. **CVE ID : CVE-2020-11546**	N/A	A-SUP-SUPE-100820/845
supremainc					
biostar_2					
Improper Limitation of a Pathname to a	7/13/2020	5	An issue was discovered in the Video Extension in Suprema BioStar 2 before	https://www.supremainc.com/en/	A-SUP-BIOS-100820/846

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			2.8.2. Remote attackers can read arbitrary files from the server via Directory Traversal. **CVE ID : CVE-2020-15050**	support/biostar-2-pakage.asp	
sylabs					
singularity					
Improper Verification of Cryptographic Signature	7/14/2020	5	Sylabs Singularity 3.0 through 3.5 has Improper Validation of an Integrity Check Value. Image integrity is not validated when an ECL policy is enforced. The fingerprint required by the ECL is compared against the signature object descriptor(s) in the SIF file, rather than to a cryptographically validated signature. **CVE ID : CVE-2020-13845**	N/A	A-SYL-SING-100820/847
N/A	7/14/2020	5	Sylabs Singularity 3.5.0 through 3.5.3 fails to report an error in a Status Code. **CVE ID : CVE-2020-13846**	N/A	A-SYL-SING-100820/848
Improper Validation of Integrity Check Value	7/14/2020	5	Sylabs Singularity 3.0 through 3.5 lacks support for an Integrity Check. Singularity's sign and verify commands do not sign metadata found in the global header or data object descriptors of a SIF file. **CVE ID : CVE-2020-13847**	N/A	A-SYL-SING-100820/849
Symantec					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
endpoint_detection_and_response					
Information Exposure	7/8/2020	5	Symantec Endpoint Detection And Response, prior to 4.4, may be susceptible to an information disclosure issue, which is a type of vulnerability that could potentially allow unauthorized access to data. **CVE ID : CVE-2020-5839**	N/A	A-SYM-ENDP-100820/850
symless					
synergy					
Improper Handling of Exceptional Conditions	7/15/2020	4	In Synergy before version 1.12.0, a Synergy server can be crashed by receiving a kMsgHelloBack packet with a client name length set to 0xffffffff (4294967295) if the servers memory is less than 4 GB. It was verified that this issue does not cause a crash through the exception handler if the available memory of the Server is more than 4GB. **CVE ID : CVE-2020-15117**	https://github.com/symless/synergy-core/security/advisories/GHSA-chfm-333q-gfpp	A-SYM-SYNE-100820/851
synacor					
zimbra_collaboration_suite					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/2/2020	4.3	An XSS vulnerability exists in the Webmail component of Zimbra Collaboration Suite before 8.8.15 Patch 11. It allows an attacker to inject executable JavaScript into the account	https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P11	A-SYN-ZIMB-100820/852

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			name of a user's profile. The injected code can be reflected and executed when changing an e-mail signature. **CVE ID : CVE-2020-13653**		
tableau					
tableau_server					
Information Exposure Through Log Files	7/8/2020	5	A sensitive information disclosure vulnerability in Tableau Server 10.5, 2018.x, 2019.x, 2020.x released before June 26, 2020, could allow access to sensitive information in log files. **CVE ID : CVE-2020-6938**	N/A	A-TAB-TABL-100820/853
telefonica					
o2_business					
URL Redirection to Untrusted Site ('Open Redirect')	7/7/2020	5.8	The O2 Business application 1.2.0 for Android exposes the canvasm.myo2.SplashActivity activity to other applications. The purpose of this activity is to handle deeplinks that can be delivered either via links or by directly calling the activity. However, the deeplink format is not properly validated. This can be abused by an attacker to redirect a user to any page and deliver any content to the user. **CVE ID : CVE-2020-11882**	N/A	A-TEL-O2_B-100820/854
Tenable					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
nessus					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/15/2020	3.5	Nessus 8.10.0 and earlier were found to contain a Stored XSS vulnerability due to improper validation of input during scan configuration. An authenticated, remote attacker could potentially exploit this vulnerability to execute arbitrary code in a user's session. Tenable has implemented additional input validation mechanisms to correct this issue in Nessus 8.11.0. **CVE ID : CVE-2020-5765**	N/A	A-TEN-NESS-100820/855
tendermint					
tendermint					
Improper Verification of Cryptographic Signature	7/2/2020	4	TenderMint from version 0.33.0 and before version 0.33.6 allows block proposers to include signatures for the wrong block. This may happen naturally if you start a network, have it run for some time and restart it (**without changing chainID**). A malicious block proposer (even with a minimal amount of stake) can use this vulnerability to completely halt the network. This issue is fixed in Tendermint 0.33.6 which checks all the signatures are for the block with 2/3+ majority before creating a	https://github.com/tendermint/tendermint/security/advisories/GHSA-6jqj-f58p-mrw3	A-TEN-TEND-100820/856

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			commit. **CVE ID : CVE-2020-15091**		
tileserver					
tileservergl					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/1/2020	4.3	An issue was discovered in server.js in TileServer GL through 3.0.0. The content of the key GET parameter is reflected unsanitized in an HTTP response for the application's main page, causing reflected XSS. **CVE ID : CVE-2020-15500**	N/A	A-TIL-TILE-100820/857
tobesoft					
xplatform					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	7/10/2020	7.5	XPLATFORM v9.2.260 and eariler versions contain a vulnerability that could allow remote files to be downloaded by setting the arguments to the vulnerable method. this can be leveraged for code execution. File download vulnerability in ___COMPONENT___ of TOBESOFT XPLATFORM allows ___ATTACKER/ATTACK____ to cause ____IMPACT____. This issue affects: TOBESOFT XPLATFORM 9.2.250 versions prior to 9.2.260 on Windows. **CVE ID : CVE-2020-7815**	N/A	A-TOB-XPLA-100820/858
Torproject					
tor					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/15/2020	4.3	Tor before 0.4.3.6 has an out-of-bounds memory access that allows a remote denial-of-service (crash) attack against Tor instances built to use Mozilla Network Security Services (NSS), aka TROVE-2020-001. **CVE ID : CVE-2020-15572**	https://blog.torproject.org/new-release-tor-03511-0428-0436-security-fixes	A-TOR-TOR-100820/859
traccar					
traccar					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	7/14/2020	4	Traccar GPS Tracking System before version 4.9 has a LDAP injection vulnerability. It occurs when user input is being used in LDAP search filter. By providing specially crafted input, an attacker can modify the logic of the LDAP query and get admin privileges. The issue only impacts instances with LDAP configuration and where users can craft their own names. This has been patched in version 4.9. **CVE ID : CVE-2020-5246**	https://github.com/traccar/traccar/security/advisories/GHSA-v955-7g22-2p49	A-TRA-TRAC-100820/860
Trendmicro					
antivirus\+_2020					
Untrusted Search Path	7/15/2020	6.9	An untrusted search path remote code execution (RCE) vulnerability in the Trend Micro Secuity 2020 (v16.0.0.1146 and below) consumer family of products could allow an attacker to run arbitrary	N/A	A-TRE-ANTI-100820/861

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code on a vulnerable system. As the Trend Micro installer tries to load DLL files from its current directory, an arbitrary DLL could also be loaded with the same privileges as the installer if run as Administrator. User interaction is required to exploit the vulnerbaility in that the target must open a malicious directory or device. **CVE ID : CVE-2020-15602**		
Out-of-bounds Read	7/15/2020	7.8	An invalid memory read vulnerability in a Trend Micro Secuity 2020 (v16.0.0.1302 and below) consumer family of products' driver could allow an attacker to manipulate the specific driver to do a system call operation with an invalid address, resulting in a potential system crash. **CVE ID : CVE-2020-15603**	N/A	A-TRE-ANTI-100820/862
internet_security_2020					
Untrusted Search Path	7/15/2020	6.9	An untrusted search path remote code execution (RCE) vulnerability in the Trend Micro Secuity 2020 (v16.0.0.1146 and below) consumer family of products could allow an attacker to run arbitrary code on a vulnerable system. As the Trend Micro installer tries to load DLL	N/A	A-TRE-INTE-100820/863

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			files from its current directory, an arbitrary DLL could also be loaded with the same privileges as the installer if run as Administrator. User interaction is required to exploit the vulnerbaility in that the target must open a malicious directory or device. **CVE ID : CVE-2020-15602**		
Out-of-bounds Read	7/15/2020	7.8	An invalid memory read vulnerability in a Trend Micro Secuity 2020 (v16.0.0.1302 and below) consumer family of products' driver could allow an attacker to manipulate the specific driver to do a system call operation with an invalid address, resulting in a potential system crash. **CVE ID : CVE-2020-15603**	N/A	A-TRE-INTE-100820/864
maximum_security_2020					
Untrusted Search Path	7/15/2020	6.9	An untrusted search path remote code execution (RCE) vulnerability in the Trend Micro Secuity 2020 (v16.0.0.1146 and below) consumer family of products could allow an attacker to run arbitrary code on a vulnerable system. As the Trend Micro installer tries to load DLL files from its current directory, an arbitrary DLL could also be loaded with	N/A	A-TRE-MAXI-100820/865

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the same privileges as the installer if run as Administrator. User interaction is required to exploit the vulnerbaility in that the target must open a malicious directory or device. **CVE ID : CVE-2020-15602**		
Out-of-bounds Read	7/15/2020	7.8	An invalid memory read vulnerability in a Trend Micro Secuity 2020 (v16.0.0.1302 and below) consumer family of products' driver could allow an attacker to manipulate the specific driver to do a system call operation with an invalid address, resulting in a potential system crash. **CVE ID : CVE-2020-15603**	N/A	A-TRE-MAXI-100820/866
premium_security_2020					
Untrusted Search Path	7/15/2020	6.9	An untrusted search path remote code execution (RCE) vulnerability in the Trend Micro Secuity 2020 (v16.0.0.1146 and below) consumer family of products could allow an attacker to run arbitrary code on a vulnerable system. As the Trend Micro installer tries to load DLL files from its current directory, an arbitrary DLL could also be loaded with the same privileges as the installer if run as Administrator. User	N/A	A-TRE-PREM-100820/867

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is required to exploit the vulnerbaility in that the target must open a malicious directory or device. **CVE ID : CVE-2020-15602**		
Out-of-bounds Read	7/15/2020	7.8	An invalid memory read vulnerability in a Trend Micro Secuity 2020 (v16.0.0.1302 and below) consumer family of products' driver could allow an attacker to manipulate the specific driver to do a system call operation with an invalid address, resulting in a potential system crash. **CVE ID : CVE-2020-15603**	N/A	A-TRE-PREM-100820/868
turn\!_project					
turn\!					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	7/7/2020	6.5	The turn extension through 0.3.2 for TYPO3 allows Remote Code Execution. **CVE ID : CVE-2020-15515**	https://typo3.org/security/advisory/typo3-ext-sa-2020-011	A-TUR-TURN-100820/869
ufactory					
xarm_studio					
N/A	7/15/2020	6.4	No authentication is required to control the robot inside the network, moreso the latest available user manual shows an option that lets the user to add a password to the	https://www.ufactory.cc/#/en/support/download/xarm	A-UFA-XARM-100820/870

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			robot but as in xarm_studio 1.3.0 the option is missing from the menu. Assuming manual control, even by forcefully removing the current operator from an active session. **CVE ID : CVE-2020-10284**		
Valvesoftware					
steam_client					
Improper Privilege Management	7/5/2020	7.2	An issue was discovered in Valve Steam Client 2.10.91.91. The installer allows local users to gain NT AUTHORITY\SYSTEM privileges because some parts of %PROGRAMFILES(X86)%\Steam and/or %COMMONPROGRAMFILES(X86)%\Steam have weak permissions during a critical time window. An attacker can make this time window arbitrarily long by using opportunistic locks. **CVE ID : CVE-2020-15530**	N/A	A-VAL-STEA-100820/871
vanguard_project					
vanguard					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/5/2020	4.3	An issue was discovered in the Vanguard plugin 2.1 for WordPress. XSS can occur via the mails/new title field, a product field to the p/ URI, or the Products Search box.	N/A	A-VAN-VANG-100820/872

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-15537		
Veeam					
veeam_availability_suite					
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/3/2020	6.5	VeeamFSR.sys in Veeam Availability Suite before 10 and Veeam Backup & Replication before 10 has no device object DACL, which allows unprivileged users to achieve total control over filesystem I/O requests. **CVE ID : CVE-2020-15518**	N/A	A-VEE-VEEA-100820/873
veeam_backup_\&_replication					
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/3/2020	6.5	VeeamFSR.sys in Veeam Availability Suite before 10 and Veeam Backup & Replication before 10 has no device object DACL, which allows unprivileged users to achieve total control over filesystem I/O requests. **CVE ID : CVE-2020-15518**	N/A	A-VEE-VEEA-100820/874
venki					
supravizio_bpm					
Improper Restriction of Excessive Authentication Attempts	7/7/2020	5	Venki Supravizio BPM 10.1.2 does not limit the number of authentication attempts. An unauthenticated user may exploit this vulnerability to launch a brute-force authentication attack against the Login page. **CVE ID : CVE-2020-15367**	N/A	A-VEN-SUPR-100820/875
Information	7/7/2020	5	A user enumeration	N/A	A-VEN-SUPR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			vulnerability flaw was found in Venki Supravizio BPM 10.1.2. This issue occurs during password recovery, where a difference in error messages could allow an attacker to determine if a username is valid or not, enabling a brute-force attack with valid usernames. **CVE ID : CVE-2020-15392**		100820/876
victor_cms_project					
victor_cms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/7/2020	4.3	Victor CMS through 2019-02-28 allows XSS via the register.php user_firstname or user_lastname field. **CVE ID : CVE-2020-15599**	https://www.exploit-db.com/exploits/48626	A-VIC-VICT-100820/877
Vmware					
remote_console					
Improper Privilege Management	7/10/2020	7.2	VMware Fusion (11.x before 11.5.5), VMware Remote Console for Mac (11.x and prior before 11.2.0) and Horizon Client for Mac (5.x and prior before 5.4.3) contain a privilege escalation vulnerability due to improper XPC Client validation. Successful exploitation of this issue may allow attackers with normal user privileges to escalate their privileges to	N/A	A-VMW-REMO-100820/878

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			root on the system where Fusion, VMware Remote Console for Mac or Horizon Client for Mac is installed. **CVE ID : CVE-2020-3974**		
fusion					
Improper Privilege Management	7/10/2020	7.2	VMware Fusion (11.x before 11.5.5), VMware Remote Console for Mac (11.x and prior before 11.2.0) and Horizon Client for Mac (5.x and prior before 5.4.3) contain a privilege escalation vulnerability due to improper XPC Client validation. Successful exploitation of this issue may allow attackers with normal user privileges to escalate their privileges to root on the system where Fusion, VMware Remote Console for Mac or Horizon Client for Mac is installed. **CVE ID : CVE-2020-3974**	N/A	A-VMW-FUSI-100820/879
velocloud_orchestrator					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	7/8/2020	6.5	The VeloCloud Orchestrator does not apply correct input validation which allows for blind SQL-injection. A malicious actor with tenant access to Velocloud Orchestrator could enter specially crafted SQL queries and obtain data to which they are not privileged.	N/A	A-VMW-VELO-100820/880

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3973		
horizon_client					
Improper Privilege Management	7/10/2020	7.2	VMware Fusion (11.x before 11.5.5), VMware Remote Console for Mac (11.x and prior before 11.2.0) and Horizon Client for Mac (5.x and prior before 5.4.3) contain a privilege escalation vulnerability due to improper XPC Client validation. Successful exploitation of this issue may allow attackers with normal user privileges to escalate their privileges to root on the system where Fusion, VMware Remote Console for Mac or Horizon Client for Mac is installed. **CVE ID : CVE-2020-3974**	N/A	A-VMW-HORI-100820/881
Webkitgtk					
webkitgtk					
Improper Input Validation	7/14/2020	7.5	The bubblewrap sandbox of WebKitGTK and WPE WebKit, prior to 2.28.3, failed to properly block access to CLONE_NEWUSER and the TIOCSTI ioctl. CLONE_NEWUSER could potentially be used to confuse xdg-desktop-portal, which allows access outside the sandbox. TIOCSTI can be used to directly execute commands outside the	https://www.openwall.com/lists/oss-security/2020/07/10/1	A-WEB-WEBK-100820/882

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sandbox by writing to the controlling terminal's input buffer, similar to CVE-2017-5226. **CVE ID : CVE-2020-13753**		
we-com					
municipality_portal_cms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/5/2020	4.3	XSS can occur in We-com Municipality portal CMS 2.1.x via the cerca/ search bar. **CVE ID : CVE-2020-15538**	N/A	A-WE--MUNI-100820/883
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	7/5/2020	7.5	SQL injection can occur in We-com Municipality portal CMS 2.1.x via the cerca/ keywords field. **CVE ID : CVE-2020-15539**	N/A	A-WE--MUNI-100820/884
opendata_cms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	7/5/2020	7.5	We-com OpenData CMS 2.0 allows SQL Injection via the username field on the administrator login page. **CVE ID : CVE-2020-15540**	N/A	A-WE--OPEN-100820/885
whoopsie_project					
whoopsie					
Allocation of Resources Without Limits or Throttling	7/6/2020	4.3	The parse_report() function in whoopsie.c in Whoopsie through 0.2.69 mishandles memory allocation failures, which	N/A	A-WHO-WHOO-100820/886

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows an attacker to cause a denial of service via a malformed crash file. **CVE ID : CVE-2020-15570**		
Wireshark					
wireshark					
Loop with Unreachable Exit Condition ('Infinite Loop')	7/5/2020	5	In Wireshark 3.2.0 to 3.2.4, the GVCP dissector could go into an infinite loop. This was addressed in epan/dissectors/packet-gvcp.c by ensuring that an offset increases in all situations. **CVE ID : CVE-2020-15466**	N/A	A-WIR-WIRE-100820/887
wpewebkit					
wpe_webkit					
Improper Input Validation	7/14/2020	7.5	The bubblewrap sandbox of WebKitGTK and WPE WebKit, prior to 2.28.3, failed to properly block access to CLONE_NEWUSER and the TIOCSTI ioctl. CLONE_NEWUSER could potentially be used to confuse xdg-desktop-portal, which allows access outside the sandbox. TIOCSTI can be used to directly execute commands outside the sandbox by writing to the controlling terminal's input buffer, similar to CVE-2017-5226. **CVE ID : CVE-2020-13753**	https://www.openwall.com/lists/oss-security/2020/07/10/1	A-WPE-WPE_-100820/888
yubico					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
libykpiv					
Out-of-bounds Read	7/9/2020	1.9	An issue was discovered in Yubico libykpiv before 2.1.0. lib/util.c in this library (which is included in yubico-piv-tool) does not properly check embedded length fields during device communication. A malicious PIV token can misreport the returned length fields during RSA key generation. This will cause stack memory to be copied into heap allocated memory that gets returned to the caller. The leaked memory could include PINs, passwords, key material, and other sensitive information depending on the integration. During further processing by the caller, this information could leak across trust boundaries. Note that RSA key generation is triggered by the host and cannot directly be triggered by the token. **CVE ID : CVE-2020-13131**	https://www.yubico.com/products/services-software/download/smart-card-drivers-tools/	A-YUB-LIBY-100820/889
Use of a Broken or Risky Cryptographic Algorithm	7/9/2020	2.1	An issue was discovered in Yubico libykpiv before 2.1.0. An attacker can trigger an incorrect free() in the ykpiv_util_generate_key() function in lib/util.c	https://www.yubico.com/support/security-advisories/ysa-2020-02/	A-YUB-LIBY-100820/890

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			through incorrect error handling code. This could be used to cause a denial of service attack. **CVE ID : CVE-2020-13132**		
piv_tool_manager					
Out-of-bounds Read	7/9/2020	1.9	An issue was discovered in Yubico libykpiv before 2.1.0. lib/util.c in this library (which is included in yubico-piv-tool) does not properly check embedded length fields during device communication. A malicious PIV token can misreport the returned length fields during RSA key generation. This will cause stack memory to be copied into heap allocated memory that gets returned to the caller. The leaked memory could include PINs, passwords, key material, and other sensitive information depending on the integration. During further processing by the caller, this information could leak across trust boundaries. Note that RSA key generation is triggered by the host and cannot directly be triggered by the token. **CVE ID : CVE-2020-13131**	https://www.yubico.com/products/services-software/download/smart-card-drivers-tools/	A-YUB-PIV_-100820/891
Use of a Broken or Risky	7/9/2020	2.1	An issue was discovered in Yubico libykpiv before	https://www.yubico.co	A-YUB-PIV_-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cryptographic Algorithm			2.1.0. An attacker can trigger an incorrect free() in the ykpiv_util_generate_key() function in lib/util.c through incorrect error handling code. This could be used to cause a denial of service attack. **CVE ID : CVE-2020-13132**	m/support/security-advisories/ysa-2020-02/	100820/892
yubikey_smart_card_minidriver					
Out-of-bounds Read	7/9/2020	1.9	An issue was discovered in Yubico libykpiv before 2.1.0. lib/util.c in this library (which is included in yubico-piv-tool) does not properly check embedded length fields during device communication. A malicious PIV token can misreport the returned length fields during RSA key generation. This will cause stack memory to be copied into heap allocated memory that gets returned to the caller. The leaked memory could include PINs, passwords, key material, and other sensitive information depending on the integration. During further processing by the caller, this information could leak across trust boundaries. Note that RSA key generation is triggered by the host and cannot	https://www.yubico.com/products/services-software/download/smart-card-drivers-tools/	A-YUB-YUBI-100820/893

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			directly be triggered by the token. **CVE ID : CVE-2020-13131**		
Use of a Broken or Risky Cryptographic Algorithm	7/9/2020	2.1	An issue was discovered in Yubico libykpiv before 2.1.0. An attacker can trigger an incorrect free() in the ykpiv_util_generate_key() function in lib/util.c through incorrect error handling code. This could be used to cause a denial of service attack. **CVE ID : CVE-2020-13132**	https://www.yubico.com/support/security-advisories/ysa-2020-02/	A-YUB-YUBI-100820/894
Hardware					
ABB					
irb140					
Insufficiently Protected Credentials	7/15/2020	7.5	The IRC5 family with UAS service enabled comes by default with credentials that can be found on publicly available manuals. ABB considers this a well documented functionality that helps customer set up however, out of our research, we found multiple production systems running these exact default credentials and consider thereby this an exposure that should be mitigated. Moreover, future deployments should consider that these defaults should be forbidden (user should be forced to change them).	https://github.com/aliasrobotics/RVD/issues/3326	H-ABB-IRB1-100820/895

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-10287		
Improper Authentication	7/15/2020	7.5	IRC5 exposes an ftp server (port 21). Upon attempting to gain access you are challenged with a request of username and password, however you can input whatever you like. As long as the field isn't empty it will be accepted. **CVE ID : CVE-2020-10288**	https://github.com/aliasrobotics/RVD/issues/3327	H-ABB-IRB1-100820/896
irc5					
Insufficiently Protected Credentials	7/15/2020	7.5	The IRC5 family with UAS service enabled comes by default with credentials that can be found on publicly available manuals. ABB considers this a well documented functionality that helps customer set up however, out of our research, we found multiple production systems running these exact default credentials and consider thereby this an exposure that should be mitigated. Moreover, future deployments should consider that these defaults should be forbidden (user should be forced to change them). **CVE ID : CVE-2020-10287**	https://github.com/aliasrobotics/RVD/issues/3326	H-ABB-IRC5-100820/897
Improper Authentication	7/15/2020	7.5	IRC5 exposes an ftp server (port 21). Upon attempting to gain access you are challenged with a request	https://github.com/aliasrobotics/RVD/issues/	H-ABB-IRC5-100820/898

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of username and password, however you can input whatever you like. As long as the field isn't empty it will be accepted. **CVE ID : CVE-2020-10288**	3327	
Cisco					
sf250-24					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the	N/A	H-CIS-SF25-100820/899

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			level of the administrative user. **CVE ID : CVE-2020-3297**		
sf250-24p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	H-CIS-SF25-100820/900
sf250-48					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	H-CIS-SF25-100820/901
sf250-48hp					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could	N/A	H-CIS-SF25-100820/902

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg250-08					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management	N/A	H-CIS-SG25-100820/903

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg250-08hp					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator	N/A	H-CIS-SG25-100820/904

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg250-10p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An	N/A	H-CIS-SG25-100820/905

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg250-18					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session	N/A	H-CIS-SG25-100820/906

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg250-26					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface	N/A	H-CIS-SG25-100820/907

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg250-26hp					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	H-CIS-SG25-100820/908

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg250-26p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	H-CIS-SG25-100820/909
sg250-50					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and	N/A	H-CIS-SG25-100820/910

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg250-50hp					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized	N/A	H-CIS-SG25-100820/911

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg250-50p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could	N/A	H-CIS-SG25-100820/912

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg250x-24					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session	N/A	H-CIS-SG25-100820/913

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg250x-24p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and	N/A	H-CIS-SG25-100820/914

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg250x-48					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the	N/A	H-CIS-SG25-100820/915

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg250x-48p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	H-CIS-SG25-100820/916

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sf350-48					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	H-CIS-SF35-100820/917
sf350-48mp					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and	N/A	H-CIS-SF35-100820/918

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf350-48p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized	N/A	H-CIS-SF35-100820/919

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg350-10					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could	N/A	H-CIS-SG35-100820/920

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg350-10mp					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session	N/A	H-CIS-SG35-100820/921

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg350-10p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and	N/A	H-CIS-SG35-100820/922

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg350-28					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the	N/A	H-CIS-SG35-100820/923

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg350-28mp					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	H-CIS-SG35-100820/924

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg350-28p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	H-CIS-SG35-100820/925
sg355-10p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and	N/A	H-CIS-SG35-100820/926

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf550x-24					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized	N/A	H-CIS-SF55-100820/927

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf550x-24mp					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could	N/A	H-CIS-SF55-100820/928

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf550x-24p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session	N/A	H-CIS-SF55-100820/929

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf550x-48					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and	N/A	H-CIS-SF55-100820/930

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf550x-48mp					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the	N/A	H-CIS-SF55-100820/931

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf550x-48p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	H-CIS-SF55-100820/932

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sf200-24					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	H-CIS-SF20-100820/933
sf200-24fp					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and	N/A	H-CIS-SF20-100820/934

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf200-24p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized	N/A	H-CIS-SF20-100820/935

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf200-48					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could	N/A	H-CIS-SF20-100820/936

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf200-48p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session	N/A	H-CIS-SF20-100820/937

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf200e-24					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and	N/A	H-CIS-SF20-100820/938

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf200e-24p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the	N/A	H-CIS-SF20-100820/939

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf200e-48					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	H-CIS-SF20-100820/940

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sf200e-48p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	H-CIS-SF20-100820/941
sg200-08					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and	N/A	H-CIS-SG20-100820/942

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg200-08p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized	N/A	H-CIS-SG20-100820/943

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg200-10fp					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could	N/A	H-CIS-SG20-100820/944

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg200-18					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session	N/A	H-CIS-SG20-100820/945

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg200-26					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and	N/A	H-CIS-SG20-100820/946

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg200-26fp					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the	N/A	H-CIS-SG20-100820/947

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg200-26p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	H-CIS-SG20-100820/948

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg200-50					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	H-CIS-SG20-100820/949
sg200-50fp					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and	N/A	H-CIS-SG20-100820/950

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg200-50p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized	N/A	H-CIS-SG20-100820/951

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf300-08					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could	N/A	H-CIS-SF30-100820/952

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf300-24					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session	N/A	H-CIS-SF30-100820/953

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf300-24mp					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and	N/A	H-CIS-SF30-100820/954

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf300-24p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the	N/A	H-CIS-SF30-100820/955

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf300-24pp					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	H-CIS-SF30-100820/956

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sf300-48					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	H-CIS-SF30-100820/957
sf300-48p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and	N/A	H-CIS-SF30-100820/958

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf300-48pp					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized	N/A	H-CIS-SF30-100820/959

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf302-08					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could	N/A	H-CIS-SF30-100820/960

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf302-08mp					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session	N/A	H-CIS-SF30-100820/961

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf302-08mpp					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and	N/A	H-CIS-SF30-100820/962

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf302-08p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the	N/A	H-CIS-SF30-100820/963

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf302-08pp					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	H-CIS-SF30-100820/964

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg300-10					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	H-CIS-SG30-100820/965
sg300-10mp					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and	N/A	H-CIS-SG30-100820/966

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg300-10mpp					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized	N/A	H-CIS-SG30-100820/967

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg300-10p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could	N/A	H-CIS-SG30-100820/968

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg300-10pp					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session	N/A	H-CIS-SG30-100820/969

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg300-10sfp					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and	N/A	H-CIS-SG30-100820/970

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg300-20					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the	N/A	H-CIS-SG30-100820/971

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg300-28					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	H-CIS-SG30-100820/972

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg300-28mp					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	H-CIS-SG30-100820/973
sg300-28p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and	N/A	H-CIS-SG30-100820/974

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg350xg-24t					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized	N/A	H-CIS-SG35-100820/975

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg350xg-2f10					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could	N/A	H-CIS-SG35-100820/976

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg350xg-48t					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session	N/A	H-CIS-SG35-100820/977

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg550x-24					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and	N/A	H-CIS-SG55-100820/978

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg550x-24mp					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the	N/A	H-CIS-SG55-100820/979

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg550x-24mpp					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	H-CIS-SG55-100820/980

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg550x-24p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	H-CIS-SG55-100820/981
sg550x-48					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and	N/A	H-CIS-SG55-100820/982

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg550x-48mp					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized	N/A	H-CIS-SG55-100820/983

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg550x-48p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could	N/A	H-CIS-SG55-100820/984

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sx550x-12f					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session	N/A	H-CIS-SX55-100820/985

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sx550x-16ft					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and	N/A	H-CIS-SX55-100820/986

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sx550x-24					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the	N/A	H-CIS-SX55-100820/987

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sx550x-24f					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	H-CIS-SX55-100820/988

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sx550x-24ft					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	H-CIS-SX55-100820/989
sx550x-52					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and	N/A	H-CIS-SX55-100820/990

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg350x-24					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized	N/A	H-CIS-SG35-100820/991

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg350x-24mp					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could	N/A	H-CIS-SG35-100820/992

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg350x-24p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session	N/A	H-CIS-SG35-100820/993

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg350x-48					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and	N/A	H-CIS-SG35-100820/994

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg350x-48mp					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the	N/A	H-CIS-SG35-100820/995

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg350x-48p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	H-CIS-SG35-100820/996

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg350xg-24f					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	H-CIS-SG35-100820/997
sg300-28pp					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and	N/A	H-CIS-SG30-100820/998

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg300-52					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized	N/A	H-CIS-SG30-100820/999

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg300-52mp					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could	N/A	H-CIS-SG30-100820/1000

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg300-52p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session	N/A	H-CIS-SG30-100820/1001

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf500-24					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and	N/A	H-CIS-SF50-100820/1002

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf500-24p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the	N/A	H-CIS-SF50-100820/1003

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf500-48					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	H-CIS-SF50-100820/1004

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sf500-48p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	H-CIS-SF50-100820/1005
sg500-28					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and	N/A	H-CIS-SG50-100820/1006

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg500-28mpp					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized	N/A	H-CIS-SG50-100820/1007

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg500-28p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could	N/A	H-CIS-SG50-100820/1008

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg500-52					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session	N/A	H-CIS-SG50-100820/1009

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg500-52mp					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and	N/A	H-CIS-SG50-100820/1010

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg500-52p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the	N/A	H-CIS-SG50-100820/1011

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg500x-24					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	H-CIS-SG50-100820/1012

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg500x-24p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	H-CIS-SG50-100820/1013
sg500x-48					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and	N/A	H-CIS-SG50-100820/1014

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg500x-48p					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized	N/A	H-CIS-SG50-100820/1015

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg500xg-8f8t					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could	N/A	H-CIS-SG50-100820/1016

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
Citrix					
netscaler_gateway					
Missing Authorization	7/10/2020	5	Improper access control in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows unauthenticated access to certain URL endpoints. **CVE ID : CVE-2020-8193**	N/A	H-CIT-NETS-100820/1017
Improper Control of Generation of Code ('Code Injection')	7/10/2020	4.3	Reflected code injection in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and	N/A	H-CIT-NETS-100820/1018

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows the modification of a file download. **CVE ID : CVE-2020-8194**		
Improper Input Validation	7/10/2020	4	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in limited information disclosure to low privileged users. **CVE ID : CVE-2020-8195**	N/A	H-CIT-NETS-100820/1019
Missing Authorization	7/10/2020	4	Improper access control in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in limited information disclosure to low privileged users. **CVE ID : CVE-2020-8196**	N/A	H-CIT-NETS-100820/1020
Improper Privilege Management	7/10/2020	6.5	Privilege escalation vulnerability on Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 allows a low privileged user with management	N/A	H-CIT-NETS-100820/1021

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to execute arbitrary commands. **CVE ID : CVE-2020-8197**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/10/2020	4.3	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in Stored Cross-Site Scripting (XSS). **CVE ID : CVE-2020-8198**	N/A	H-CIT-NETS-100820/1022
Improper Input Validation	7/10/2020	5	Improper input validation in Citrix ADC and Citrix Gateway versions before 11.1-63.9 and 12.0-62.10 allows unauthenticated users to perform a denial of service attack. **CVE ID : CVE-2020-8187**	N/A	H-CIT-NETS-100820/1023
Improper Preservation of Permissions	7/10/2020	6	Incorrect file permissions in Citrix ADC and Citrix Gateway before versions 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 allows privilege escalation. **CVE ID : CVE-2020-8190**	N/A	H-CIT-NETS-100820/1024
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/10/2020	4.3	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows reflected	N/A	H-CIT-NETS-100820/1025

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cross Site Scripting (XSS). **CVE ID : CVE-2020-8191**		
application_delivery_controller					
Missing Authorization	7/10/2020	5	Improper access control in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows unauthenticated access to certain URL endpoints. **CVE ID : CVE-2020-8193**	N/A	H-CIT-APPL-100820/1026
Improper Control of Generation of Code ('Code Injection')	7/10/2020	4.3	Reflected code injection in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows the modification of a file download. **CVE ID : CVE-2020-8194**	N/A	H-CIT-APPL-100820/1027
Improper Input Validation	7/10/2020	4	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in limited information disclosure to low privileged users.	N/A	H-CIT-APPL-100820/1028

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8195		
Missing Authorization	7/10/2020	4	Improper access control in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in limited information disclosure to low privileged users. **CVE ID : CVE-2020-8196**	N/A	H-CIT-APPL-100820/1029
Improper Privilege Management	7/10/2020	6.5	Privilege escalation vulnerability on Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 allows a low privileged user with management access to execute arbitrary commands. **CVE ID : CVE-2020-8197**	N/A	H-CIT-APPL-100820/1030
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/10/2020	4.3	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in Stored Cross-Site Scripting (XSS). **CVE ID : CVE-2020-8198**	N/A	H-CIT-APPL-100820/1031
Improper Input Validation	7/10/2020	5	Improper input validation in Citrix ADC and Citrix Gateway before 11.1-63.9 and 12.0-62.10	N/A	H-CIT-APPL-100820/1032

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows unauthenticated users to perform a denial of service attack. **CVE ID : CVE-2020-8187**		
Improper Preservation of Permissions	7/10/2020	6	Incorrect file permissions in Citrix ADC and Citrix Gateway before versions 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 allows privilege escalation. **CVE ID : CVE-2020-8190**	N/A	H-CIT-APPL-100820/1033
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/10/2020	4.3	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows reflected Cross Site Scripting (XSS). **CVE ID : CVE-2020-8191**	N/A	H-CIT-APPL-100820/1034
gateway					
Missing Authorization	7/10/2020	5	Improper access control in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows unauthenticated access to certain URL endpoints. **CVE ID : CVE-2020-8193**	N/A	H-CIT-GATE-100820/1035
Improper Control of	7/10/2020	4.3	Reflected code injection in Citrix ADC and Citrix	N/A	H-CIT-GATE-100820/1036

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation of Code ('Code Injection')			Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows the modification of a file download. **CVE ID : CVE-2020-8194**		
Improper Input Validation	7/10/2020	4	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in limited information disclosure to low privileged users. **CVE ID : CVE-2020-8195**	N/A	H-CIT-GATE-100820/1037
Missing Authorization	7/10/2020	4	Improper access control in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in limited information disclosure to low privileged users. **CVE ID : CVE-2020-8196**	N/A	H-CIT-GATE-100820/1038
Improper Privilege Management	7/10/2020	6.5	Privilege escalation vulnerability on Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21,	N/A	H-CIT-GATE-100820/1039

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			11.1-64.14 and 10.5-70.18 allows a low privileged user with management access to execute arbitrary commands. **CVE ID : CVE-2020-8197**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/10/2020	4.3	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in Stored Cross-Site Scripting (XSS). **CVE ID : CVE-2020-8198**	N/A	H-CIT-GATE-100820/1040
Improper Preservation of Permissions	7/10/2020	6	Incorrect file permissions in Citrix ADC and Citrix Gateway before versions 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 allows privilege escalation. **CVE ID : CVE-2020-8190**	N/A	H-CIT-GATE-100820/1041
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/10/2020	4.3	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows reflected Cross Site Scripting (XSS). **CVE ID : CVE-2020-8191**	N/A	H-CIT-GATE-100820/1042
4000-wo					
Missing	7/10/2020	5	Improper access control in	N/A	H-CIT-4000-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authorization			Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows unauthenticated access to certain URL endpoints. **CVE ID : CVE-2020-8193**		100820/1043
Improper Control of Generation of Code ('Code Injection')	7/10/2020	4.3	Reflected code injection in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows the modification of a file download. **CVE ID : CVE-2020-8194**	N/A	H-CIT-4000-100820/1044
Improper Input Validation	7/10/2020	4	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in limited information disclosure to low privileged users. **CVE ID : CVE-2020-8195**	N/A	H-CIT-4000-100820/1045
Missing Authorization	7/10/2020	4	Improper access control in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18,	N/A	H-CIT-4000-100820/1046

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in limited information disclosure to low privileged users. **CVE ID : CVE-2020-8196**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/10/2020	4.3	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in Stored Cross-Site Scripting (XSS). **CVE ID : CVE-2020-8198**	N/A	H-CIT-4000-100820/1047
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/10/2020	4.3	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows reflected Cross Site Scripting (XSS). **CVE ID : CVE-2020-8191**	N/A	H-CIT-4000-100820/1048
4100-wo					
Missing Authorization	7/10/2020	5	Improper access control in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and	N/A	H-CIT-4100-100820/1049

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.2.7 allows unauthenticated access to certain URL endpoints. **CVE ID : CVE-2020-8193**		
Improper Control of Generation of Code ('Code Injection')	7/10/2020	4.3	Reflected code injection in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows the modification of a file download. **CVE ID : CVE-2020-8194**	N/A	H-CIT-4100-100820/1050
Improper Input Validation	7/10/2020	4	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in limited information disclosure to low privileged users. **CVE ID : CVE-2020-8195**	N/A	H-CIT-4100-100820/1051
Missing Authorization	7/10/2020	4	Improper access control in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in limited information disclosure to low privileged users.	N/A	H-CIT-4100-100820/1052

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8196		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/10/2020	4.3	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in Stored Cross-Site Scripting (XSS). **CVE ID : CVE-2020-8198**	N/A	H-CIT-4100-100820/1053
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/10/2020	4.3	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows reflected Cross Site Scripting (XSS). **CVE ID : CVE-2020-8191**	N/A	H-CIT-4100-100820/1054
5000-wo					
Missing Authorization	7/10/2020	5	Improper access control in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows unauthenticated access to certain URL endpoints. **CVE ID : CVE-2020-8193**	N/A	H-CIT-5000-100820/1055
Improper Control of Generation of	7/10/2020	4.3	Reflected code injection in Citrix ADC and Citrix Gateway versions before	N/A	H-CIT-5000-100820/1056

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Code ('Code Injection')			13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows the modification of a file download. **CVE ID : CVE-2020-8194**		
Improper Input Validation	7/10/2020	4	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in limited information disclosure to low privileged users. **CVE ID : CVE-2020-8195**	N/A	H-CIT-5000-100820/1057
Missing Authorization	7/10/2020	4	Improper access control in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in limited information disclosure to low privileged users. **CVE ID : CVE-2020-8196**	N/A	H-CIT-5000-100820/1058
Improper Neutralization of Input During Web Page Generation ('Cross-site	7/10/2020	4.3	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix	N/A	H-CIT-5000-100820/1059

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in Stored Cross-Site Scripting (XSS). **CVE ID : CVE-2020-8198**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/10/2020	4.3	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows reflected Cross Site Scripting (XSS). **CVE ID : CVE-2020-8191**	N/A	H-CIT-5000-100820/1060
5100-wo					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/10/2020	4.3	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows reflected Cross Site Scripting (XSS). **CVE ID : CVE-2020-8191**	N/A	H-CIT-5100-100820/1061
Missing Authorization	7/10/2020	5	Improper access control in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows unauthenticated access to certain URL endpoints.	N/A	H-CIT-5100-100820/1062

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8193		
Improper Control of Generation of Code ('Code Injection')	7/10/2020	4.3	Reflected code injection in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows the modification of a file download. **CVE ID : CVE-2020-8194**	N/A	H-CIT-5100-100820/1063
Improper Input Validation	7/10/2020	4	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in limited information disclosure to low privileged users. **CVE ID : CVE-2020-8195**	N/A	H-CIT-5100-100820/1064
Missing Authorization	7/10/2020	4	Improper access control in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in limited information disclosure to low privileged users. **CVE ID : CVE-2020-8196**	N/A	H-CIT-5100-100820/1065
Improper Neutralization	7/10/2020	4.3	Improper input validation in Citrix ADC and Citrix	N/A	H-CIT-5100-100820/1066

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input During Web Page Generation ('Cross-site Scripting')			Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in Stored Cross-Site Scripting (XSS). **CVE ID : CVE-2020-8198**		
Dell					
vxrail_d560f					
Missing Authorization	7/6/2020	5	Dell EMC VxRail versions 4.7.410 and 4.7.411 contain an improper authentication vulnerability. A remote unauthenticated attacker may exploit this vulnerability to obtain sensitive information in an encrypted form. **CVE ID : CVE-2020-5368**	N/A	H-DEL-VXRA-100820/1067
vxrail_d560					
Missing Authorization	7/6/2020	5	Dell EMC VxRail versions 4.7.410 and 4.7.411 contain an improper authentication vulnerability. A remote unauthenticated attacker may exploit this vulnerability to obtain sensitive information in an encrypted form. **CVE ID : CVE-2020-5368**	N/A	H-DEL-VXRA-100820/1068
emc_powerstore_1000					
Incorrect Authorization	7/6/2020	5	Dell EMC PowerStore versions prior to 1.0.1.0.5.002 contain a	N/A	H-DEL-EMC_-100820/1069

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability that exposes test interface ports to external network. A remote unauthenticated attacker could potentially cause Denial of Service via test interface ports which are not used during run time environment. **CVE ID : CVE-2020-5372**		
emc_powerstore_3000					
Incorrect Authorization	7/6/2020	5	Dell EMC PowerStore versions prior to 1.0.1.0.5.002 contain a vulnerability that exposes test interface ports to external network. A remote unauthenticated attacker could potentially cause Denial of Service via test interface ports which are not used during run time environment. **CVE ID : CVE-2020-5372**	N/A	H-DEL-EMC_-100820/1070
emc_powerstore_5000					
Incorrect Authorization	7/6/2020	5	Dell EMC PowerStore versions prior to 1.0.1.0.5.002 contain a vulnerability that exposes test interface ports to external network. A remote unauthenticated attacker could potentially cause Denial of Service via test interface ports which are not used during run time environment. **CVE ID : CVE-2020-5372**	N/A	H-DEL-EMC_-100820/1071

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
emc_powerstore_7000					
Incorrect Authorization	7/6/2020	5	Dell EMC PowerStore versions prior to 1.0.1.0.5.002 contain a vulnerability that exposes test interface ports to external network. A remote unauthenticated attacker could potentially cause Denial of Service via test interface ports which are not used during run time environment. **CVE ID : CVE-2020-5372**	N/A	H-DEL-EMC_-100820/1072
emc_powerstore_9000					
Incorrect Authorization	7/6/2020	5	Dell EMC PowerStore versions prior to 1.0.1.0.5.002 contain a vulnerability that exposes test interface ports to external network. A remote unauthenticated attacker could potentially cause Denial of Service via test interface ports which are not used during run time environment. **CVE ID : CVE-2020-5372**	N/A	H-DEL-EMC_-100820/1073
powerprotect_x400					
Files or Directories Accessible to External Parties	7/6/2020	4	Dell PowerProtect Data Manager (PPDM) versions prior to 19.4 and Dell PowerProtect X400 versions prior to 3.2 contain an improper authorization vulnerability. A remote authenticated malicious user may download any	N/A	H-DEL-POWE-100820/1074

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			file from the affected PowerProtect virtual machines. **CVE ID : CVE-2020-5356**		
idrac9					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	7/9/2020	4	Dell EMC iDRAC9 versions prior to 4.20.20.20 contain a Path Traversal Vulnerability. A remote authenticated malicious user with low privileges could potentially exploit this vulnerability by manipulating input parameters to gain unauthorized read access to the arbitrary files. **CVE ID : CVE-2020-5366**	N/A	H-DEL-IDRA-100820/1075
Dlink					
dir-610					
Information Exposure	7/9/2020	5	** UNSUPPORTED WHEN ASSIGNED ** D-Link DIR-610 devices allow Information Disclosure via SERVICES=DEVICE.ACCOUNT%0AAUTHORIZED_GROUP=1 to getcfg.php. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2020-9376**	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10182	H-DLI-DIR--100820/1076
Improper Control of Generation of Code ('Code Injection')	7/9/2020	6.5	** UNSUPPORTED WHEN ASSIGNED ** D-Link DIR-610 devices allow Remote Command Execution via the cmd parameter to command.php. NOTE: This	https://supportannouncement.us.dlink.com/announcement/publicatio	H-DLI-DIR--100820/1077

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2020-9377**	n.aspx?name=SAP10182	
Geovision					
gv-as210					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/8/2020	7.5	Buffer overflow exists in Geovision Door Access Control device family, an unauthenticated remote attacker can execute arbitrary command. **CVE ID : CVE-2020-3931**	https://www.acronis.com/en-us/blog/posts/backdoor-wide-open-critical-vulnerabilities-uncovered-geovision, https://www.twcert.org.tw/tw/cp-132-3754-b77d0-1.html	H-GEO-GV-A-100820/1078
gv-as410					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/8/2020	7.5	Buffer overflow exists in Geovision Door Access Control device family, an unauthenticated remote attacker can execute arbitrary command. **CVE ID : CVE-2020-3931**	https://www.acronis.com/en-us/blog/posts/backdoor-wide-open-critical-vulnerabilities-uncovered-geovision, https://ww	H-GEO-GV-A-100820/1079

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				w.twcert.org.tw/tw/cp-132-3754-b77d0-1.html	
gv-as810					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/8/2020	7.5	Buffer overflow exists in Geovision Door Access Control device family, an unauthenticated remote attacker can execute arbitrary command. **CVE ID : CVE-2020-3931**	https://www.acronis.com/en-us/blog/posts/backdoor-wide-open-critical-vulnerabilities-uncovered-geovision, https://www.twcert.org.tw/tw/cp-132-3754-b77d0-1.html	H-GEO-GV-A-100820/1080
gv-gf1921					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/8/2020	7.5	Buffer overflow exists in Geovision Door Access Control device family, an unauthenticated remote attacker can execute arbitrary command. **CVE ID : CVE-2020-3931**	https://www.acronis.com/en-us/blog/posts/backdoor-wide-open-critical-vulnerabilities-uncovered-geovision, https://www.twcert.org.tw/tw/cp-	H-GEO-GV-G-100820/1081

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				132-3754-b77d0-1.html	
gv-as1010					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/8/2020	7.5	Buffer overflow exists in Geovision Door Access Control device family, an unauthenticated remote attacker can execute arbitrary command. **CVE ID : CVE-2020-3931**	https://www.acronis.com/en-us/blog/posts/backdoor-wide-open-critical-vulnerabilities-uncovered-geovision, https://www.twcert.org.tw/tw/cp-132-3754-b77d0-1.html	H-GEO-GV-A-100820/1082
gv-gf1922					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/8/2020	7.5	Buffer overflow exists in Geovision Door Access Control device family, an unauthenticated remote attacker can execute arbitrary command. **CVE ID : CVE-2020-3931**	https://www.acronis.com/en-us/blog/posts/backdoor-wide-open-critical-vulnerabilities-uncovered-geovision, https://www.twcert.org.tw/tw/cp-132-3754-b77d0-	H-GEO-GV-G-100820/1083

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				1.html	
gpononu					
1ge_router_wifi_onu_v2801rw					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	7/15/2020	9	Guangzhou 1GE ONU V2801RW 1.9.1-181203 through 2.9.0-181024 and V2804RGW 1.9.1-181203 through 2.9.0-181024 devices allow remote attackers to execute arbitrary OS commands via shell metacharacters in the boaform/admin/formPing Dest IP Address field. **CVE ID : CVE-2020-8958**	N/A	H-GPO-1GE_-100820/1084
1ge\+3fe\+wifi_onu_v2804rgw					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	7/15/2020	9	Guangzhou 1GE ONU V2801RW 1.9.1-181203 through 2.9.0-181024 and V2804RGW 1.9.1-181203 through 2.9.0-181024 devices allow remote attackers to execute arbitrary OS commands via shell metacharacters in the boaform/admin/formPing Dest IP Address field. **CVE ID : CVE-2020-8958**	N/A	H-GPO-1GE\-100820/1085
Huawei					
mate_30_pro					
Improper Authentication	7/6/2020	1.9	HUAWEI Mate 30 Pro with versions earlier than 10.1.0.150(C00E136R5P3) have is an improper authentication vulnerability. The device does not sufficiently validate certain credential	N/A	H-HUA-MATE-100820/1086

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of user's face, an attacker could craft the credential of the user, successful exploit could allow the attacker to pass the authentication with the crafted credential. **CVE ID : CVE-2020-1838**		
changxiang_8_plus					
Improper Input Validation	7/6/2020	2.9	ChangXiang 8 Plus with versions earlier than 9.1.0.136(C00E121R1P6T8) have a denial of service vulnerability. The device does not properly handle certain message from base station, the attacker could craft a fake base station to launch the attack. Successful exploit could cause a denial of signal service condition. **CVE ID : CVE-2020-1837**	N/A	H-HUA-CHAN-100820/1087
p30_pro					
Information Exposure	7/6/2020	2.9	HUAWEI P30 with versions earlier than 10.1.0.160(C00E160R2P11) and HUAWEI P30 Pro with versions earlier than 10.1.0.160(C00E160R2P8) have an information disclosure vulnerability. Certain function's default configuration in the system seems insecure, an attacker should craft a WI-FI hotspot to launch the attack. Successful exploit could cause information	N/A	H-HUA-P30_-100820/1088

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disclosure. **CVE ID : CVE-2020-1836**		
Information Exposure	7/10/2020	3.3	HUAWEI P30 and HUAWEI P30 Pro smartphones with versions earlier than 10.1.0.123(C432E22R2P5) and versions earlier than 10.1.0.160(C00E160R2P8) have an information disclosure vulnerability. Certain WI-FI function's default configuration in the system seems insecure, an attacker should craft a WI-FI hotspot to launch the attack. Successful exploit could cause information disclosure. **CVE ID : CVE-2020-9260**	N/A	H-HUA-P30_-100820/1089
p30					
Information Exposure	7/6/2020	2.9	HUAWEI P30 with versions earlier than 10.1.0.160(C00E160R2P11) and HUAWEI P30 Pro with versions earlier than 10.1.0.160(C00E160R2P8) have an information disclosure vulnerability. Certain function's default configuration in the system seems insecure, an attacker should craft a WI-FI hotspot to launch the attack. Successful exploit could cause information disclosure. **CVE ID : CVE-2020-1836**	N/A	H-HUA-P30-100820/1090
Improper Verification of	7/6/2020	4.3	HUAWEI P30 with versions earlier than	N/A	H-HUA-P30-100820/1091

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cryptographic Signature			10.1.0.135(C00E135R2P11) have an improper signature verification vulnerability. The system does not improper check signature of specific software package, an attacker may exploit this vulnerability to load a crafted software package to the device. **CVE ID : CVE-2020-9226**		
Information Exposure	7/10/2020	1.9	HUAWEI P30 smartphone with versions earlier than 10.1.0.135(C00E135R2P11) have an improper input verification vulnerability. An attribution in a module is not set correctly and some verification is lacked. Attackers with local access can exploit this vulnerability by injecting malicious fragment. This may lead to user information leak. **CVE ID : CVE-2020-9258**	N/A	H-HUA-P30-100820/1092
Information Exposure	7/10/2020	3.3	HUAWEI P30 and HUAWEI P30 Pro smartphones with versions earlier than 10.1.0.123(C432E22R2P5) and versions earlier than 10.1.0.160(C00E160R2P8) have an information disclosure vulnerability. Certain WI-FI function's default configuration in the system seems insecure, an attacker should craft a WI-FI hotspot to launch the	N/A	H-HUA-P30-100820/1093

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attack. Successful exploit could cause information disclosure. **CVE ID : CVE-2020-9260**		
mate_30					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	7/6/2020	3.7	HUAWEI Mate 30 with versions earlier than 10.1.0.150(C00E136R5P3) have a race condition vulnerability. There is a timing window exists in which certain pointer members can be modified by another process that is operating concurrently, an attacker should trick the user into running a crafted application with high privilege, successful exploit could cause code execution. **CVE ID : CVE-2020-1839**	N/A	H-HUA-MATE-100820/1094
Access of Resource Using Incompatible Type ('Type Confusion')	7/6/2020	6.8	HUAWEI Mate 30 with versions earlier than 10.1.0.150(C00E136R5P3) have a type confusion vulnerability. The system does not properly check and transform the type of certain variable, the attacker tricks the user into installing then running a crafted application, successful exploit could cause code execution. **CVE ID : CVE-2020-9261**	N/A	H-HUA-MATE-100820/1095
Use After Free	7/6/2020	6.8	HUAWEI Mate 30 with versions earlier than	N/A	H-HUA-MATE-100820/1096

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.1.0.150(C00E136R5P3) have a use after free vulnerability. There is a condition exists that the system would reference memory after it has been freed, the attacker should trick the user into running a crafted application with high privilege, successful exploit could cause code execution. **CVE ID : CVE-2020-9262**		
Mitsubishielectric					
got2000_gt23					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/7/2020	7.5	TCP/IP function included in the firmware of Mitsubishi Electric GOT2000 series (CoreOS with version -Y and earlier installed in GT27 Model, GT25 Model, and GT23 Model) contains a buffer overflow vulnerability, which may allow a remote attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet. **CVE ID : CVE-2020-5595**	N/A	H-MIT-GOT2-100820/1097
Session Fixation	7/7/2020	5	TCP/IP function included in the firmware of Mitsubishi Electric GOT2000 series (CoreOS with version -Y and earlier installed in GT27 Model, GT25 Model, and GT23 Model) does not properly	N/A	H-MIT-GOT2-100820/1098

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			manage sessions, which may allow a remote attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet. **CVE ID : CVE-2020-5596**		
NULL Pointer Dereference	7/7/2020	5	TCP/IP function included in the firmware of Mitsubishi Electric GOT2000 series (CoreOS with version -Y and earlier installed in GT27 Model, GT25 Model, and GT23 Model) contains a null pointer dereference vulnerability, which may allow a remote attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet. **CVE ID : CVE-2020-5597**	N/A	H-MIT-GOT2-100820/1099
Incorrect Authorization	7/7/2020	5	TCP/IP function included in the firmware of Mitsubishi Electric GOT2000 series (CoreOS with version -Y and earlier installed in GT27 Model, GT25 Model, and GT23 Model) contains an improper access control vulnerability, which may which may allow a remote attacker tobypass access restriction and stop the network functions of the products or execute a malicious program via a	N/A	H-MIT-GOT2-100820/1100

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specially crafted packet. **CVE ID : CVE-2020-5598**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	7/7/2020	10	TCP/IP function included in the firmware of Mitsubishi Electric GOT2000 series (CoreOS with version -Y and earlier installed in GT27 Model, GT25 Model, and GT23 Model) contains an improper neutralization of argument delimiters in a command ('Argument Injection') vulnerability, which may allow a remote attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet. **CVE ID : CVE-2020-5599**	N/A	H-MIT-GOT2-100820/1101
Uncontrolled Resource Consumption	7/7/2020	5	TCP/IP function included in the firmware of Mitsubishi Electric GOT2000 series (CoreOS with version -Y and earlier installed in GT27 Model, GT25 Model, and GT23 Model) contains a resource management error vulnerability, which may allow a remote attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet. **CVE ID : CVE-2020-5600**	N/A	H-MIT-GOT2-100820/1102
got2000_gt25					
Buffer Copy	7/7/2020	7.5	TCP/IP function included	N/A	H-MIT-GOT2-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			in the firmware of Mitsubishi Electric GOT2000 series (CoreOS with version -Y and earlier installed in GT27 Model, GT25 Model, and GT23 Model) contains a buffer overflow vulnerability, which may allow a remote attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet. **CVE ID : CVE-2020-5595**		100820/1103
Session Fixation	7/7/2020	5	TCP/IP function included in the firmware of Mitsubishi Electric GOT2000 series (CoreOS with version -Y and earlier installed in GT27 Model, GT25 Model, and GT23 Model) does not properly manage sessions, which may allow a remote attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet. **CVE ID : CVE-2020-5596**	N/A	H-MIT-GOT2-100820/1104
NULL Pointer Dereference	7/7/2020	5	TCP/IP function included in the firmware of Mitsubishi Electric GOT2000 series (CoreOS with version -Y and earlier installed in GT27 Model, GT25 Model, and GT23 Model) contains a null pointer dereference	N/A	H-MIT-GOT2-100820/1105

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, which may allow a remote attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet. **CVE ID : CVE-2020-5597**		
Incorrect Authorization	7/7/2020	5	TCP/IP function included in the firmware of Mitsubishi Electric GOT2000 series (CoreOS with version -Y and earlier installed in GT27 Model, GT25 Model, and GT23 Model) contains an improper access control vulnerability, which may which may allow a remote attacker tobypass access restriction and stop the network functions of the products or execute a malicious program via a specially crafted packet. **CVE ID : CVE-2020-5598**	N/A	H-MIT-GOT2-100820/1106
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	7/7/2020	10	TCP/IP function included in the firmware of Mitsubishi Electric GOT2000 series (CoreOS with version -Y and earlier installed in GT27 Model, GT25 Model, and GT23 Model) contains an improper neutralization of argument delimiters in a command ('Argument Injection') vulnerability, which may allow a remote attacker to stop the network functions of the	N/A	H-MIT-GOT2-100820/1107

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			products or execute a malicious program via a specially crafted packet. **CVE ID : CVE-2020-5599**		
Uncontrolled Resource Consumption	7/7/2020	5	TCP/IP function included in the firmware of Mitsubishi Electric GOT2000 series (CoreOS with version -Y and earlier installed in GT27 Model, GT25 Model, and GT23 Model) contains a resource management error vulnerability, which may allow a remote attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet. **CVE ID : CVE-2020-5600**	N/A	H-MIT-GOT2-100820/1108
got2000_gt27					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/7/2020	7.5	TCP/IP function included in the firmware of Mitsubishi Electric GOT2000 series (CoreOS with version -Y and earlier installed in GT27 Model, GT25 Model, and GT23 Model) contains a buffer overflow vulnerability, which may allow a remote attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet. **CVE ID : CVE-2020-5595**	N/A	H-MIT-GOT2-100820/1109
Session Fixation	7/7/2020	5	TCP/IP function included in the firmware of	N/A	H-MIT-GOT2-100820/1110

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mitsubishi Electric GOT2000 series (CoreOS with version -Y and earlier installed in GT27 Model, GT25 Model, and GT23 Model) does not properly manage sessions, which may allow a remote attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet. **CVE ID : CVE-2020-5596**		
NULL Pointer Dereference	7/7/2020	5	TCP/IP function included in the firmware of Mitsubishi Electric GOT2000 series (CoreOS with version -Y and earlier installed in GT27 Model, GT25 Model, and GT23 Model) contains a null pointer dereference vulnerability, which may allow a remote attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet. **CVE ID : CVE-2020-5597**	N/A	H-MIT-GOT2-100820/1111
Incorrect Authorization	7/7/2020	5	TCP/IP function included in the firmware of Mitsubishi Electric GOT2000 series (CoreOS with version -Y and earlier installed in GT27 Model, GT25 Model, and GT23 Model) contains an improper access control vulnerability, which may	N/A	H-MIT-GOT2-100820/1112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which may allow a remote attacker tobypass access restriction and stop the network functions of the products or execute a malicious program via a specially crafted packet. **CVE ID : CVE-2020-5598**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	7/7/2020	10	TCP/IP function included in the firmware of Mitsubishi Electric GOT2000 series (CoreOS with version -Y and earlier installed in GT27 Model, GT25 Model, and GT23 Model) contains an improper neutralization of argument delimiters in a command ('Argument Injection') vulnerability, which may allow a remote attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet. **CVE ID : CVE-2020-5599**	N/A	H-MIT-GOT2-100820/1113
Uncontrolled Resource Consumption	7/7/2020	5	TCP/IP function included in the firmware of Mitsubishi Electric GOT2000 series (CoreOS with version -Y and earlier installed in GT27 Model, GT25 Model, and GT23 Model) contains a resource management error vulnerability, which may allow a remote attacker to stop the network functions of the products or execute	N/A	H-MIT-GOT2-100820/1114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a malicious program via a specially crafted packet. **CVE ID : CVE-2020-5600**		
Moxa					
edr-g902-t					
Out-of-bounds Write	7/15/2020	7.5	Malicious operation of the crafted web browser cookie may cause a stack-based buffer overflow in the system web server on the EDR-G902 and EDR-G903 Series Routers (versions prior to 5.4). **CVE ID : CVE-2020-14511**	N/A	H-MOX-EDR--100820/1115
edr-g902					
Out-of-bounds Write	7/15/2020	7.5	Malicious operation of the crafted web browser cookie may cause a stack-based buffer overflow in the system web server on the EDR-G902 and EDR-G903 Series Routers (versions prior to 5.4). **CVE ID : CVE-2020-14511**	N/A	H-MOX-EDR--100820/1116
edr-g903-t					
Out-of-bounds Write	7/15/2020	7.5	Malicious operation of the crafted web browser cookie may cause a stack-based buffer overflow in the system web server on the EDR-G902 and EDR-G903 Series Routers (versions prior to 5.4). **CVE ID : CVE-2020-14511**	N/A	H-MOX-EDR--100820/1117
edr-g903					
Out-of-bounds Write	7/15/2020	7.5	Malicious operation of the crafted web browser	N/A	H-MOX-EDR--100820/1118

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cookie may cause a stack-based buffer overflow in the system web server on the EDR-G902 and EDR-G903 Series Routers (versions prior to 5.4). **CVE ID : CVE-2020-14511**		
Realtek					
rtl8711am					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/6/2020	4.9	An issue was discovered on Realtek RTL8195AM, RTL8711AM, RTL8711AF, and RTL8710AF devices before 2.0.6. A stack-based buffer overflow exists in the client code that takes care of WPA2's 4-way-handshake via a malformed EAPOL-Key packet with a long keydata buffer. **CVE ID : CVE-2020-9395**	N/A	H-REA-RTL8-100820/1119
rtl8195am					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/6/2020	4.9	An issue was discovered on Realtek RTL8195AM, RTL8711AM, RTL8711AF, and RTL8710AF devices before 2.0.6. A stack-based buffer overflow exists in the client code that takes care of WPA2's 4-way-handshake via a malformed EAPOL-Key packet with a long keydata buffer. **CVE ID : CVE-2020-9395**	N/A	H-REA-RTL8-100820/1120
rtl8710af					
Buffer Copy	7/6/2020	4.9	An issue was discovered	N/A	H-REA-RTL8-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			on Realtek RTL8195AM, RTL8711AM, RTL8711AF, and RTL8710AF devices before 2.0.6. A stack-based buffer overflow exists in the client code that takes care of WPA2's 4-way-handshake via a malformed EAPOL-Key packet with a long keydata buffer. **CVE ID : CVE-2020-9395**		100820/1121
rtl8711af					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/6/2020	4.9	An issue was discovered on Realtek RTL8195AM, RTL8711AM, RTL8711AF, and RTL8710AF devices before 2.0.6. A stack-based buffer overflow exists in the client code that takes care of WPA2's 4-way-handshake via a malformed EAPOL-Key packet with a long keydata buffer. **CVE ID : CVE-2020-9395**	N/A	H-REA-RTL8-100820/1122
rittal					
cmciii-pu-9333e0fb					
Use of Hard-coded Credentials	7/14/2020	10	An issue was discovered on Rittal PDU-3C002DEC through 5.17.10 and CMCIII-PU-9333E0FB through 3.17.10 devices. There is a Backdoor root account. **CVE ID : CVE-2020-11951**	N/A	H-RIT-CMCI-100820/1123
Information Exposure	7/14/2020	4.9	An issue was discovered on Rittal PDU-3C002DEC	N/A	H-RIT-CMCI-100820/1124

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			through 5.17.10 and CMCIII-PU-9333E0FB through 3.17.10 devices. Attackers can bypass the CLI menu. **CVE ID : CVE-2020-11952**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	7/14/2020	9	An issue was discovered on Rittal PDU-3C002DEC through 5.15.40 and CMCIII-PU-9333E0FB through 3.15.70_4 devices. Attackers can execute code. **CVE ID : CVE-2020-11953**	N/A	H-RIT-CMCI-100820/1125
Incorrect Default Permissions	7/14/2020	9	An issue was discovered on Rittal PDU-3C002DEC through 5.15.70 and CMCIII-PU-9333E0FB through 3.15.70 devices. There are insecure permissions. **CVE ID : CVE-2020-11955**	N/A	H-RIT-CMCI-100820/1126
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	7/14/2020	10	An issue was discovered on Rittal PDU-3C002DEC through 5.17.10 and CMCIII-PU-9333E0FB through 3.17.10 devices. There is a least privilege violation. **CVE ID : CVE-2020-11956**	N/A	H-RIT-CMCI-100820/1127
pdu-3c002dec					
Use of Hard-coded Credentials	7/14/2020	10	An issue was discovered on Rittal PDU-3C002DEC through 5.17.10 and CMCIII-PU-9333E0FB through 3.17.10 devices. There is a Backdoor root account.	N/A	H-RIT-PDU--100820/1128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-11951		
Information Exposure	7/14/2020	4.9	An issue was discovered on Rittal PDU-3C002DEC through 5.17.10 and CMCIII-PU-9333E0FB through 3.17.10 devices. Attackers can bypass the CLI menu. **CVE ID : CVE-2020-11952**	N/A	H-RIT-PDU--100820/1129
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	7/14/2020	9	An issue was discovered on Rittal PDU-3C002DEC through 5.15.40 and CMCIII-PU-9333E0FB through 3.15.70_4 devices. Attackers can execute code. **CVE ID : CVE-2020-11953**	N/A	H-RIT-PDU--100820/1130
Incorrect Default Permissions	7/14/2020	9	An issue was discovered on Rittal PDU-3C002DEC through 5.15.70 and CMCIII-PU-9333E0FB through 3.15.70 devices. There are insecure permissions. **CVE ID : CVE-2020-11955**	N/A	H-RIT-PDU--100820/1131
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	7/14/2020	10	An issue was discovered on Rittal PDU-3C002DEC through 5.17.10 and CMCIII-PU-9333E0FB through 3.17.10 devices. There is a least privilege violation. **CVE ID : CVE-2020-11956**	N/A	H-RIT-PDU--100820/1132
cmc_iii_pu_7030.000					
Use of Hard-coded Credentials	7/14/2020	10	An issue was discovered on Rittal PDU-3C002DEC through 5.17.10 and CMCIII-PU-9333E0FB	N/A	H-RIT-CMC_-100820/1133

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			through 3.17.10 devices. There is a Backdoor root account. **CVE ID : CVE-2020-11951**		
Information Exposure	7/14/2020	4.9	An issue was discovered on Rittal PDU-3C002DEC through 5.17.10 and CMCIII-PU-9333E0FB through 3.17.10 devices. Attackers can bypass the CLI menu. **CVE ID : CVE-2020-11952**	N/A	H-RIT-CMC_-100820/1134
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	7/14/2020	9	An issue was discovered on Rittal PDU-3C002DEC through 5.15.40 and CMCIII-PU-9333E0FB through 3.15.70_4 devices. Attackers can execute code. **CVE ID : CVE-2020-11953**	N/A	H-RIT-CMC_-100820/1135
Incorrect Default Permissions	7/14/2020	9	An issue was discovered on Rittal PDU-3C002DEC through 5.15.70 and CMCIII-PU-9333E0FB through 3.15.70 devices. There are insecure permissions. **CVE ID : CVE-2020-11955**	N/A	H-RIT-CMC_-100820/1136
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	7/14/2020	10	An issue was discovered on Rittal PDU-3C002DEC through 5.17.10 and CMCIII-PU-9333E0FB through 3.17.10 devices. There is a least privilege violation. **CVE ID : CVE-2020-11956**	N/A	H-RIT-CMC_-100820/1137
lcp-cw					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	7/14/2020	10	An issue was discovered on Rittal PDU-3C002DEC through 5.17.10 and CMCIII-PU-9333E0FB through 3.17.10 devices. There is a Backdoor root account. **CVE ID : CVE-2020-11951**	N/A	H-RIT-LCP--100820/1138
Information Exposure	7/14/2020	4.9	An issue was discovered on Rittal PDU-3C002DEC through 5.17.10 and CMCIII-PU-9333E0FB through 3.17.10 devices. Attackers can bypass the CLI menu. **CVE ID : CVE-2020-11952**	N/A	H-RIT-LCP--100820/1139
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	7/14/2020	9	An issue was discovered on Rittal PDU-3C002DEC through 5.15.40 and CMCIII-PU-9333E0FB through 3.15.70_4 devices. Attackers can execute code. **CVE ID : CVE-2020-11953**	N/A	H-RIT-LCP--100820/1140
Incorrect Default Permissions	7/14/2020	9	An issue was discovered on Rittal PDU-3C002DEC through 5.15.70 and CMCIII-PU-9333E0FB through 3.15.70 devices. There are insecure permissions. **CVE ID : CVE-2020-11955**	N/A	H-RIT-LCP--100820/1141
Improper Neutralization of Special Elements used in an OS Command ('OS Command	7/14/2020	10	An issue was discovered on Rittal PDU-3C002DEC through 5.17.10 and CMCIII-PU-9333E0FB through 3.17.10 devices. There is a least privilege	N/A	H-RIT-LCP--100820/1142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			violation. **CVE ID : CVE-2020-11956**		
Samsung					
exynos_7885					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/7/2020	4.3	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) (Exynos 7885 chipsets) software. The Bluetooth Low Energy (BLE) component has a buffer overflow with a resultant deadlock or crash. The Samsung ID is SVE-2020-16870 (July 2020). **CVE ID : CVE-2020-15582**	https://security.samsungmobile.com/securityUpdate.smsb	H-SAM-EXYN-100820/1143
Siemens					
sicam_mmu					
Out-of-bounds Read	7/14/2020	5	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). By performing a flooding attack against the web server, an attacker might be able to gain read access to the device's memory, possibly revealing confidential information. **CVE ID : CVE-2020-10037**	N/A	H-SIE-SICA-100820/1144
Missing Authentication for Critical Function	7/14/2020	7.5	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions <	N/A	H-SIE-SICA-100820/1145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V2.18). An attacker with access to the device's web server might be able to execute administrative commands without authentication. **CVE ID : CVE-2020-10038**		
Missing Encryption of Sensitive Data	7/14/2020	6.8	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). An attacker in a privileged network position between a legitimate user and the web server might be able to conduct a Man-in-the-middle attack and gain read and write access to the transmitted data. **CVE ID : CVE-2020-10039**	N/A	H-SIE-SICA-100820/1146
Use of Password Hash With Insufficient Computational Effort	7/14/2020	2.1	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). An attacker with local access to the device might be able to retrieve some passwords in clear text. **CVE ID : CVE-2020-10040**	N/A	H-SIE-SICA-100820/1147
Improper Neutralization of Input During Web Page Generation ('Cross-site	7/14/2020	4.3	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). A stored Cross-	N/A	H-SIE-SICA-100820/1148

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			Site-Scripting (XSS) vulnerability is present in different locations of the web application. An attacker might be able to take over a session of a legitimate user. **CVE ID : CVE-2020-10041**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/14/2020	7.5	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). A buffer overflow in various positions of the web application might enable an attacker with access to the web application to execute arbitrary code over the network. **CVE ID : CVE-2020-10042**	N/A	H-SIE-SICA-100820/1149
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/14/2020	4.3	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). The web server could allow Cross-Site Scripting (XSS) attacks if unsuspecting users are tricked into accessing a malicious link. **CVE ID : CVE-2020-10043**	N/A	H-SIE-SICA-100820/1150
Missing Authentication for Critical Function	7/14/2020	5	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions <	N/A	H-SIE-SICA-100820/1151

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V2.18). An attacker with access to the network could be able to install specially crafted firmware to the device. **CVE ID : CVE-2020-10044**		
Authentication Bypass by Capture-replay	7/14/2020	6.8	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). An error in the challenge-response procedure could allow an attacker to replay authentication traffic and gain access to protected areas of the web application. **CVE ID : CVE-2020-10045**	N/A	H-SIE-SICA-100820/1152
sicam_sgu					
Out-of-bounds Read	7/14/2020	5	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). By performing a flooding attack against the web server, an attacker might be able to gain read access to the device's memory, possibly revealing confidential information. **CVE ID : CVE-2020-10037**	N/A	H-SIE-SICA-100820/1153
Missing Authentication for Critical Function	7/14/2020	7.5	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions),	N/A	H-SIE-SICA-100820/1154

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SICAM T (All versions < V2.18). An attacker with access to the device's web server might be able to execute administrative commands without authentication. **CVE ID : CVE-2020-10038**		
Missing Encryption of Sensitive Data	7/14/2020	6.8	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). An attacker in a privileged network position between a legitimate user and the web server might be able to conduct a Man-in-the-middle attack and gain read and write access to the transmitted data. **CVE ID : CVE-2020-10039**	N/A	H-SIE-SICA-100820/1155
Use of Password Hash With Insufficient Computational Effort	7/14/2020	2.1	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). An attacker with local access to the device might be able to retrieve some passwords in clear text. **CVE ID : CVE-2020-10040**	N/A	H-SIE-SICA-100820/1156
Improper Neutralization of Input During Web Page Generation	7/14/2020	4.3	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions <	N/A	H-SIE-SICA-100820/1157

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			V2.18). A stored Cross-Site-Scripting (XSS) vulnerability is present in different locations of the web application. An attacker might be able to take over a session of a legitimate user. **CVE ID : CVE-2020-10041**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/14/2020	7.5	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). A buffer overflow in various positions of the web application might enable an attacker with access to the web application to execute arbitrary code over the network. **CVE ID : CVE-2020-10042**	N/A	H-SIE-SICA-100820/1158
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/14/2020	4.3	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). The web server could allow Cross-Site Scripting (XSS) attacks if unsuspecting users are tricked into accessing a malicious link. **CVE ID : CVE-2020-10043**	N/A	H-SIE-SICA-100820/1159
Missing Authentication for Critical Function	7/14/2020	5	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions),	N/A	H-SIE-SICA-100820/1160

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SICAM T (All versions < V2.18). An attacker with access to the network could be able to install specially crafted firmware to the device. **CVE ID : CVE-2020-10044**		
Authentication Bypass by Capture-replay	7/14/2020	6.8	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). An error in the challenge-response procedure could allow an attacker to replay authentication traffic and gain access to protected areas of the web application. **CVE ID : CVE-2020-10045**	N/A	H-SIE-SICA-100820/1161
sicam_t					
Out-of-bounds Read	7/14/2020	5	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). By performing a flooding attack against the web server, an attacker might be able to gain read access to the device's memory, possibly revealing confidential information. **CVE ID : CVE-2020-10037**	N/A	H-SIE-SICA-100820/1162
Missing Authentication for Critical	7/14/2020	7.5	A vulnerability has been identified in SICAM MMU (All versions < V2.05),	N/A	H-SIE-SICA-100820/1163

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Function			SICAM SGU (All versions), SICAM T (All versions < V2.18). An attacker with access to the device's web server might be able to execute administrative commands without authentication. **CVE ID : CVE-2020-10038**		
Missing Encryption of Sensitive Data	7/14/2020	6.8	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). An attacker in a privileged network position between a legitimate user and the web server might be able to conduct a Man-in-the-middle attack and gain read and write access to the transmitted data. **CVE ID : CVE-2020-10039**	N/A	H-SIE-SICA-100820/1164
Use of Password Hash With Insufficient Computational Effort	7/14/2020	2.1	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). An attacker with local access to the device might be able to retrieve some passwords in clear text. **CVE ID : CVE-2020-10040**	N/A	H-SIE-SICA-100820/1165
Improper Neutralization of Input During Web Page	7/14/2020	4.3	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions),	N/A	H-SIE-SICA-100820/1166

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			SICAM T (All versions < V2.18). A stored Cross-Site-Scripting (XSS) vulnerability is present in different locations of the web application. An attacker might be able to take over a session of a legitimate user. **CVE ID : CVE-2020-10041**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/14/2020	7.5	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). A buffer overflow in various positions of the web application might enable an attacker with access to the web application to execute arbitrary code over the network. **CVE ID : CVE-2020-10042**	N/A	H-SIE-SICA-100820/1167
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/14/2020	4.3	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). The web server could allow Cross-Site Scripting (XSS) attacks if unsuspecting users are tricked into accessing a malicious link. **CVE ID : CVE-2020-10043**	N/A	H-SIE-SICA-100820/1168
Missing Authentication for Critical	7/14/2020	5	A vulnerability has been identified in SICAM MMU (All versions < V2.05),	N/A	H-SIE-SICA-100820/1169

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Function			SICAM SGU (All versions), SICAM T (All versions < V2.18). An attacker with access to the network could be able to install specially crafted firmware to the device. **CVE ID : CVE-2020-10044**		
Authentication Bypass by Capture-replay	7/14/2020	6.8	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). An error in the challenge-response procedure could allow an attacker to replay authentication traffic and gain access to protected areas of the web application. **CVE ID : CVE-2020-10045**	N/A	H-SIE-SICA-100820/1170
logo\!_8_bm					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/14/2020	7.5	A vulnerability has been identified in LOGO! 8 BM (incl. SIPLUS variants) (V1.81.01 - V1.81.03), LOGO! 8 BM (incl. SIPLUS variants) (V1.82.01), LOGO! 8 BM (incl. SIPLUS variants) (V1.82.02). A buffer overflow vulnerability exists in the Web Server functionality of the device. A remote unauthenticated attacker could send a specially crafted HTTP request to cause a memory corruption, potentially	N/A	H-SIE-LOGO-100820/1171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resulting in remote code execution. **CVE ID : CVE-2020-7593**		
simatic_hmi_comfort_panels					
Cleartext Transmission of Sensitive Information	7/14/2020	3.3	A vulnerability has been identified in SIMATIC HMI Basic Panels 1st Generation (incl. SIPLUS variants) (All versions), SIMATIC HMI Basic Panels 2nd Generation (incl. SIPLUS variants) (All versions), SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions), SIMATIC HMI KTP700F Mobile Arctic (All versions), SIMATIC HMI Mobile Panels 2nd Generation (All versions), SIMATIC WinCC Runtime Advanced (All versions). Unencrypted communication between the configuration software and the respective device could allow an attacker to capture potential plain text communication and have access to sensitive information. **CVE ID : CVE-2020-7592**	N/A	H-SIE-SIMA-100820/1172
simatic_hmi_ktp700f_mobile_arctic					
Cleartext Transmission of Sensitive Information	7/14/2020	3.3	A vulnerability has been identified in SIMATIC HMI Basic Panels 1st Generation (incl. SIPLUS variants) (All versions), SIMATIC HMI Basic Panels	N/A	H-SIE-SIMA-100820/1173

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2nd Generation (incl. SIPLUS variants) (All versions), SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions), SIMATIC HMI KTP700F Mobile Arctic (All versions), SIMATIC HMI Mobile Panels 2nd Generation (All versions), SIMATIC WinCC Runtime Advanced (All versions). Unencrypted communication between the configuration software and the respective device could allow an attacker to capture potential plain text communication and have access to sensitive information. **CVE ID : CVE-2020-7592**		
simatic_hmi_mobile_panels_2nd_generation					
Cleartext Transmission of Sensitive Information	7/14/2020	3.3	A vulnerability has been identified in SIMATIC HMI Basic Panels 1st Generation (incl. SIPLUS variants) (All versions), SIMATIC HMI Basic Panels 2nd Generation (incl. SIPLUS variants) (All versions), SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions), SIMATIC HMI KTP700F Mobile Arctic (All versions), SIMATIC HMI Mobile Panels 2nd Generation (All versions), SIMATIC WinCC Runtime	N/A	H-SIE-SIMA-100820/1174

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Advanced (All versions). Unencrypted communication between the configuration software and the respective device could allow an attacker to capture potential plain text communication and have access to sensitive information. **CVE ID : CVE-2020-7592**		
simatic_s7-200_smart_sr_cpu					
Uncontrolled Resource Consumption	7/14/2020	5	A vulnerability has been identified in SIMATIC S7-200 SMART CPU family (All versions >= V2.2 < V2.5.1). Affected devices do not properly handle large numbers of new incomming connections and could crash under certain circumstances. An attacker may leverage this to cause a Denial-of-Service situation. **CVE ID : CVE-2020-7584**	N/A	H-SIE-SIMA-100820/1175
simatic_s7-200_smart_st_cpu					
Uncontrolled Resource Consumption	7/14/2020	5	A vulnerability has been identified in SIMATIC S7-200 SMART CPU family (All versions >= V2.2 < V2.5.1). Affected devices do not properly handle large numbers of new incomming connections and could crash under certain circumstances. An attacker may leverage this to cause a Denial-of-	N/A	H-SIE-SIMA-100820/1176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service situation. **CVE ID : CVE-2020-7584**		
Tenda					
ac15					
Cross-Site Request Forgery (CSRF)	7/13/2020	7.1	A CSRF issue in the /goform/SysToolReboot endpoint of Tenda AC15 AC1900 version 15.03.05.19 allows remote attackers to reboot the device and cause denial of service via a payload hosted by an attacker-controlled web page. **CVE ID : CVE-2020-10986**	N/A	H-TEN-AC15-100820/1177
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	7/13/2020	10	The goform/setUsbUnload endpoint of Tenda AC15 AC1900 version 15.03.05.19 allows remote attackers to execute arbitrary system commands via the deviceName POST parameter. **CVE ID : CVE-2020-10987**	N/A	H-TEN-AC15-100820/1178
Use of Hard-coded Credentials	7/13/2020	10	A hard-coded telnet credential in the tenda_login binary of Tenda AC15 AC1900 version 15.03.05.19 allows unauthenticated remote attackers to start a telnetd service on the device. **CVE ID : CVE-2020-10988**	N/A	H-TEN-AC15-100820/1179
Improper Neutralization of Input During Web Page	7/13/2020	4.3	An XSS issue in the /goform/WifiBasicSet endpoint of Tenda AC15 AC1900 version	N/A	H-TEN-AC15-100820/1180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			15.03.05.19 allows remote attackers to execute malicious payloads via the WifiName POST parameter. **CVE ID : CVE-2020-10989**		
ufactory					
xarm_5_lite					
Improper Restriction of Excessive Authentication Attempts	7/15/2020	7.5	The authentication implementation on the xArm controller has very low entropy, making it vulnerable to a brute-force attack. There is no mechanism in place to mitigate or lockout automated attempts to gain access. **CVE ID : CVE-2020-10285**	https://github.com/aliasrobotics/RVD/issues/3322	H-UFA-XARM-100820/1181
N/A	7/15/2020	5.8	the main user account has restricted privileges but is in the sudoers group and there is not any mechanism in place to prevent sudo su or sudo -i to be run gaining unrestricted access to sensible files, encryption, or issue orders that disrupt robot operation. **CVE ID : CVE-2020-10286**	https://github.com/aliasrobotics/RVD/issues/3323	H-UFA-XARM-100820/1182
xarm_6					
N/A	7/15/2020	5.8	the main user account has restricted privileges but is in the sudoers group and there is not any mechanism in place to prevent sudo su or sudo -i	https://github.com/aliasrobotics/RVD/issues/3323	H-UFA-XARM-100820/1183

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to be run gaining unrestricted access to sensible files, encryption, or issue orders that disrupt robot operation. **CVE ID : CVE-2020-10286**		
xarm_7					
N/A	7/15/2020	5.8	the main user account has restricted privileges but is in the sudoers group and there is not any mechanism in place to prevent sudo su or sudo -i to be run gaining unrestricted access to sensible files, encryption, or issue orders that disrupt robot operation. **CVE ID : CVE-2020-10286**	https://github.com/aliasrobotics/RVD/issues/3323	H-UFA-XARM-100820/1184
ui					
unifi_protect					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	7/2/2020	6.5	We have recently released new version of UniFi Protect firmware v1.13.3 and v1.14.10 for Unifi Cloud Key Gen2 Plus and UniFi Dream Machine Pro/UNVR respectively that fixes vulnerabilities found on Protect firmware v1.13.2, v1.14.9 and prior according to the description below:View only users can run certain custom commands which allows them to assign themselves unauthorized roles and escalate their privileges.	N/A	H-UI-UNIF-100820/1185

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8188		
unifi_cloud_key_plus					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	7/2/2020	6.5	We have recently released new version of UniFi Protect firmware v1.13.3 and v1.14.10 for Unifi Cloud Key Gen2 Plus and UniFi Dream Machine Pro/UNVR respectively that fixes vulnerabilities found on Protect firmware v1.13.2, v1.14.9 and prior according to the description below:View only users can run certain custom commands which allows them to assign themselves unauthorized roles and escalate their privileges. **CVE ID : CVE-2020-8188**	N/A	H-UI-UNIF-100820/1186
unifi_dream_machine_pro					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	7/2/2020	6.5	We have recently released new version of UniFi Protect firmware v1.13.3 and v1.14.10 for Unifi Cloud Key Gen2 Plus and UniFi Dream Machine Pro/UNVR respectively that fixes vulnerabilities found on Protect firmware v1.13.2, v1.14.9 and prior according to the description below:View only users can run certain custom commands which allows them to assign themselves unauthorized roles and escalate their	N/A	H-UI-UNIF-100820/1187

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges. **CVE ID : CVE-2020-8188**		
wavlink					
wl-wn530hg4					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	7/1/2020	10	An issue was discovered on Wavlink WL-WN530HG4 M30HG4.V5030.191116 devices. Multiple shell metacharacter injection vulnerabilities exist in CGI scripts, leading to remote code execution with root privileges. **CVE ID : CVE-2020-15489**	N/A	H-WAV-WL-W-100820/1188
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/1/2020	10	An issue was discovered on Wavlink WL-WN530HG4 M30HG4.V5030.191116 devices. Multiple buffer overflow vulnerabilities exist in CGI scripts, leading to remote code execution with root privileges. (The set of affected scripts is similar to CVE-2020-12266.) **CVE ID : CVE-2020-15490**	N/A	H-WAV-WL-W-100820/1189
yubico					
yubikey_5_nfc					
N/A	7/9/2020	4.3	A PIN management problem was discovered on Yubico YubiKey 5 devices 5.2.0 to 5.2.6. OpenPGP has three passwords: Admin PIN, Reset Code, and User PIN. The Reset Code is used to	https://www.yubico.com/support/security-advisories/ysa-2020-05/	H-YUB-YUBI-100820/1190

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reset the User PIN, but it is disabled by default. A flaw in the implementation of OpenPGP sets the Reset Code to a known value upon initialization. If the retry counter for the Reset Code is set to non-zero without changing the Reset Code, this known value can be used to reset the User PIN. To set the retry counters, the Admin PIN is required. **CVE ID : CVE-2020-15000**		
Information Exposure	7/9/2020	2.9	An information leak was discovered on Yubico YubiKey 5 NFC devices 5.0.0 to 5.2.6 and 5.3.0 to 5.3.1. The OTP application allows a user to set optional access codes on OTP slots. This access code is intended to prevent unauthorized changes to OTP configurations. The access code is not checked when updating NFC specific components of the OTP configurations. This may allow an attacker to access configured OTPs and passwords stored in slots that were not configured by the user to be read over NFC, despite a user having set an access code. (Users who have not set an access code, or who have not configured the OTP slots, are not	https://www.yubico.com/support/security-advisories/ysa-2020-04/	H-YUB-YUBI-100820/1191

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			impacted by this issue.) **CVE ID : CVE-2020-15001**		
Operating System					
ABB					
irb140_firmware					
Insufficiently Protected Credentials	7/15/2020	7.5	The IRC5 family with UAS service enabled comes by default with credentials that can be found on publicly available manuals. ABB considers this a well documented functionality that helps customer set up however, out of our research, we found multiple production systems running these exact default credentials and consider thereby this an exposure that should be mitigated. Moreover, future deployments should consider that these defaults should be forbidden (user should be forced to change them). **CVE ID : CVE-2020-10287**	https://github.com/aliasrobotics/RVD/issues/3326	O-ABB-IRB1-100820/1192
irc5_firmware					
Insufficiently Protected Credentials	7/15/2020	7.5	The IRC5 family with UAS service enabled comes by default with credentials that can be found on publicly available manuals. ABB considers this a well documented functionality that helps customer set up however, out of our research, we found multiple production	https://github.com/aliasrobotics/RVD/issues/3326	O-ABB-IRC5-100820/1193

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			systems running these exact default credentials and consider thereby this an exposure that should be mitigated. Moreover, future deployments should consider that these defaults should be forbidden (user should be forced to change them). **CVE ID : CVE-2020-10287**		
Apple					
mac_os					
N/A	7/15/2020	4.4	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.44, prior to 6.0.24 and prior to 6.1.12. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. Note: The CVE-2020-14711 is applicable to macOS host only. CVSS 3.1 Base Score 6.5 (Confidentiality, Integrity and Availability	N/A	O-APP-MAC_-100820/1194

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2020-14711**		
Improper Privilege Management	7/10/2020	7.2	VMware Fusion (11.x before 11.5.5), VMware Remote Console for Mac (11.x and prior before 11.2.0) and Horizon Client for Mac (5.x and prior before 5.4.3) contain a privilege escalation vulnerability due to improper XPC Client validation. Successful exploitation of this issue may allow attackers with normal user privileges to escalate their privileges to root on the system where Fusion, VMware Remote Console for Mac or Horizon Client for Mac is installed. **CVE ID : CVE-2020-3974**	N/A	O-APP-MAC_-100820/1195
Canonical					
ubuntu_linux					
Use After Free	7/6/2020	4	A use-after-free flaw was found in all samba LDAP server versions before 4.10.17, before 4.11.11, before 4.12.4 used in a AC DC configuration. A Samba LDAP user could use this flaw to crash samba. **CVE ID : CVE-2020-10760**	N/A	O-CAN-UBUN-100820/1196
Cisco					
sf302-08pp_firmware					
Improper	7/2/2020	10	A vulnerability in session	N/A	O-CIS-SF30-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication			management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		100820/1197
sf302-08mpp_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated,	N/A	O-CIS-SF30-100820/1198

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf300-24_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker	N/A	O-CIS-SF30-100820/1199

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf300-24p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device.	N/A	O-CIS-SF30-100820/1200

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf300-24mp_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this	N/A	O-CIS-SF30-100820/1201

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf300-24pp_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an	N/A	O-CIS-SF30-100820/1202

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf300-48_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the	N/A	O-CIS-SF30-100820/1203

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			level of the administrative user. **CVE ID : CVE-2020-3297**		
sf300-48p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	O-CIS-SF30-100820/1204
sf300-48pp_firmware					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	O-CIS-SF30-100820/1205
sf500-24_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could	N/A	O-CIS-SF50-100820/1206

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf500-24p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management	N/A	O-CIS-SF50-100820/1207

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf500-48_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator	N/A	O-CIS-SF50-100820/1208

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf500-48p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An	N/A	O-CIS-SF50-100820/1209

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg500-28_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session	N/A	O-CIS-SG50-100820/1210

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg500-28p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface	N/A	O-CIS-SG50-100820/1211

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg500-28mpp_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	O-CIS-SG50-100820/1212

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg500-52_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	O-CIS-SG50-100820/1213
sg500-52p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and	N/A	O-CIS-SG50-100820/1214

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg500-52mp_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized	N/A	O-CIS-SG50-100820/1215

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg500x-24_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could	N/A	O-CIS-SG50-100820/1216

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg500x-48_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session	N/A	O-CIS-SG50-100820/1217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg500x-48p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and	N/A	O-CIS-SG50-100820/1218

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg250x-24_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the	N/A	O-CIS-SG25-100820/1219

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg250x-24p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	O-CIS-SG25-100820/1220

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg250x-48_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	O-CIS-SG25-100820/1221
sg250x-48p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and	N/A	O-CIS-SG25-100820/1222

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg250-08_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized	N/A	O-CIS-SG25-100820/1223

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg250-08hp_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could	N/A	O-CIS-SG25-100820/1224

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg250-10p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session	N/A	O-CIS-SG25-100820/1225

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg250-18_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and	N/A	O-CIS-SG25-100820/1226

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg250-26_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the	N/A	O-CIS-SG25-100820/1227

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg250-26hp_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	O-CIS-SG25-100820/1228

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg250-26p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	O-CIS-SG25-100820/1229
sg250-50_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and	N/A	O-CIS-SG25-100820/1230

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg250-50hp_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized	N/A	O-CIS-SG25-100820/1231

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg250-50p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could	N/A	O-CIS-SG25-100820/1232

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf350-48_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session	N/A	O-CIS-SF35-100820/1233

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf350-48p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and	N/A	O-CIS-SF35-100820/1234

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf350-48mp_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the	N/A	O-CIS-SF35-100820/1235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg350-10_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	O-CIS-SG35-100820/1236

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg350-10p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	O-CIS-SG35-100820/1237
sg350-10mp_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and	N/A	O-CIS-SG35-100820/1238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg350-28_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized	N/A	O-CIS-SG35-100820/1239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg350-28p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could	N/A	O-CIS-SG35-100820/1240

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg350-28mp_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session	N/A	O-CIS-SG35-100820/1241

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sx550x-16ft_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and	N/A	O-CIS-SX55-100820/1242

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sx550x-24ft_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the	N/A	O-CIS-SX55-100820/1243

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sx550x-24_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	O-CIS-SX55-100820/1244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sx550x-52_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	O-CIS-SX55-100820/1245
sg550x-24_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and	N/A	O-CIS-SG55-100820/1246

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg550x-24p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized	N/A	O-CIS-SG55-100820/1247

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg550x-24mp_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could	N/A	O-CIS-SG55-100820/1248

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg550x-24mpp_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session	N/A	O-CIS-SG55-100820/1249

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg550x-48_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and	N/A	O-CIS-SG55-100820/1250

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg550x-48p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the	N/A	O-CIS-SG55-100820/1251

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg550x-48mp_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	O-CIS-SG55-100820/1252

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sf200-24_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	O-CIS-SF20-100820/1253
sf200-24p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and	N/A	O-CIS-SF20-100820/1254

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf200-48_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized	N/A	O-CIS-SF20-100820/1255

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf200-48p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could	N/A	O-CIS-SF20-100820/1256

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg200-18_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session	N/A	O-CIS-SG20-100820/1257

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg200-26_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and	N/A	O-CIS-SG20-100820/1258

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg200-26p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the	N/A	O-CIS-SG20-100820/1259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg200-50_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	O-CIS-SG20-100820/1260

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg200-50p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	O-CIS-SG20-100820/1261
sg300-10_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and	N/A	O-CIS-SG30-100820/1262

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg300-10mp_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized	N/A	O-CIS-SG30-100820/1263

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg300-10mpp_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could	N/A	O-CIS-SG30-100820/1264

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg300-10sfp_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session	N/A	O-CIS-SG30-100820/1265

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg300-10p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and	N/A	O-CIS-SG30-100820/1266

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg300-10pp_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the	N/A	O-CIS-SG30-100820/1267

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg300-20_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	O-CIS-SG30-100820/1268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg300-28_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	O-CIS-SG30-100820/1269
sg300-28p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and	N/A	O-CIS-SG30-100820/1270

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg300-28pp_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized	N/A	O-CIS-SG30-100820/1271

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg300-28mp_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could	N/A	O-CIS-SG30-100820/1272

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg300-52_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session	N/A	O-CIS-SG30-100820/1273

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg300-52p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and	N/A	O-CIS-SG30-100820/1274

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg300-52mp_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the	N/A	O-CIS-SG30-100820/1275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf300-08_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	O-CIS-SF30-100820/1276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sf302-08_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	O-CIS-SF30-100820/1277
sf302-08mp_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and	N/A	O-CIS-SF30-100820/1278

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf302-08p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized	N/A	O-CIS-SF30-100820/1279

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf550x-24_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could	N/A	O-CIS-SF55-100820/1280

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf550x-24p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session	N/A	O-CIS-SF55-100820/1281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf550x-48_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and	N/A	O-CIS-SF55-100820/1282

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf550x-48p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the	N/A	O-CIS-SF55-100820/1283

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf550x-48mp_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	O-CIS-SF55-100820/1284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg200-50fp_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	O-CIS-SG20-100820/1285
sg200-26fp_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and	N/A	O-CIS-SG20-100820/1286

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg200-10fp_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized	N/A	O-CIS-SG20-100820/1287

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg200-08_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could	N/A	O-CIS-SG20-100820/1288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg200-08p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session	N/A	O-CIS-SG20-100820/1289

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf200-24fp_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and	N/A	O-CIS-SF20-100820/1290

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg500xg-8f8t_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the	N/A	O-CIS-SG50-100820/1291

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg500x-24p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	O-CIS-SG50-100820/1292

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sf250-24_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	O-CIS-SF25-100820/1293
sf250-24p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and	N/A	O-CIS-SF25-100820/1294

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf250-48_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized	N/A	O-CIS-SF25-100820/1295

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf250-48hp_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could	N/A	O-CIS-SF25-100820/1296

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg355-10p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session	N/A	O-CIS-SG35-100820/1297

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg350xg-2f10_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and	N/A	O-CIS-SG35-100820/1298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg350xg-24f_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the	N/A	O-CIS-SG35-100820/1299

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg350xg-24t_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	O-CIS-SG35-100820/1300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg350xg-48t_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	O-CIS-SG35-100820/1301
sg350x-24_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and	N/A	O-CIS-SG35-100820/1302

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg350x-24p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized	N/A	O-CIS-SG35-100820/1303

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg350x-24mp_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could	N/A	O-CIS-SG35-100820/1304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg350x-48_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session	N/A	O-CIS-SG35-100820/1305

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg350x-48p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and	N/A	O-CIS-SG35-100820/1306

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sg350x-48mp_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the	N/A	O-CIS-SG35-100820/1307

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sx550x-12f_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	O-CIS-SX55-100820/1308

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sx550x-24f_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**	N/A	O-CIS-SX55-100820/1309
sf550x-24mp_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and	N/A	O-CIS-SF55-100820/1310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf200e-24_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized	N/A	O-CIS-SF20-100820/1311

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf200e-24p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could	N/A	O-CIS-SF20-100820/1312

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf200e-48_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session	N/A	O-CIS-SF20-100820/1313

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
sf200e-48p_firmware					
Improper Authentication	7/2/2020	10	A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. The attacker could obtain the privileges of the highjacked session account, which could include administrator privileges on the device. The vulnerability is due to the use of weak entropy generation for session identifier values. An attacker could exploit this vulnerability to determine a current session identifier through brute force and	N/A	O-CIS-SF20-100820/1314

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reuse that session identifier to take over an ongoing session. In this way, an attacker could take actions within the management interface with privileges up to the level of the administrative user. **CVE ID : CVE-2020-3297**		
Citrix					
application_delivery_controller_firmware					
Missing Authorization	7/10/2020	5	Improper access control in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows unauthenticated access to certain URL endpoints. **CVE ID : CVE-2020-8193**	N/A	O-CIT-APPL-100820/1315
Improper Control of Generation of Code ('Code Injection')	7/10/2020	4.3	Reflected code injection in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows the modification of a file download. **CVE ID : CVE-2020-8194**	N/A	O-CIT-APPL-100820/1316
Improper Input Validation	7/10/2020	4	Improper input validation in Citrix ADC and Citrix Gateway versions before	N/A	O-CIT-APPL-100820/1317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in limited information disclosure to low privileged users. **CVE ID : CVE-2020-8195**		
Missing Authorization	7/10/2020	4	Improper access control in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in limited information disclosure to low privileged users. **CVE ID : CVE-2020-8196**	N/A	O-CIT-APPL-100820/1318
Improper Privilege Management	7/10/2020	6.5	Privilege escalation vulnerability on Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 allows a low privileged user with management access to execute arbitrary commands. **CVE ID : CVE-2020-8197**	N/A	O-CIT-APPL-100820/1319
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/10/2020	4.3	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions	N/A	O-CIT-APPL-100820/1320

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 11.1.1a, 11.0.3d and 10.2.7 resulting in Stored Cross-Site Scripting (XSS). **CVE ID : CVE-2020-8198**		
Improper Input Validation	7/10/2020	5	Improper input validation in Citrix ADC and Citrix Gateway versions before 11.1-63.9 and 12.0-62.10 allows unauthenticated users to perform a denial of service attack. **CVE ID : CVE-2020-8187**	N/A	O-CIT-APPL-100820/1321
Improper Preservation of Permissions	7/10/2020	6	Incorrect file permissions in Citrix ADC and Citrix Gateway before versions 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 allows privilege escalation. **CVE ID : CVE-2020-8190**	N/A	O-CIT-APPL-100820/1322
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/10/2020	4.3	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows reflected Cross Site Scripting (XSS). **CVE ID : CVE-2020-8191**	N/A	O-CIT-APPL-100820/1323
gateway_firmware					
Missing Authorization	7/10/2020	5	Improper access control in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix	N/A	O-CIT-GATE-100820/1324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows unauthenticated access to certain URL endpoints. **CVE ID : CVE-2020-8193**		
Improper Control of Generation of Code ('Code Injection')	7/10/2020	4.3	Reflected code injection in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows the modification of a file download. **CVE ID : CVE-2020-8194**	N/A	O-CIT-GATE-100820/1325
Improper Input Validation	7/10/2020	4	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in limited information disclosure to low privileged users. **CVE ID : CVE-2020-8195**	N/A	O-CIT-GATE-100820/1326
Missing Authorization	7/10/2020	4	Improper access control in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in limited	N/A	O-CIT-GATE-100820/1327

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure to low privileged users. **CVE ID : CVE-2020-8196**		
Improper Privilege Management	7/10/2020	6.5	Privilege escalation vulnerability on Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 allows a low privileged user with management access to execute arbitrary commands. **CVE ID : CVE-2020-8197**	N/A	O-CIT-GATE-100820/1328
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/10/2020	4.3	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in Stored Cross-Site Scripting (XSS). **CVE ID : CVE-2020-8198**	N/A	O-CIT-GATE-100820/1329
Improper Preservation of Permissions	7/10/2020	6	Incorrect file permissions in Citrix ADC and Citrix Gateway before versions 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 allows privilege escalation. **CVE ID : CVE-2020-8190**	N/A	O-CIT-GATE-100820/1330
Improper Neutralization of Input During Web Page Generation ('Cross-site	7/10/2020	4.3	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix	N/A	O-CIT-GATE-100820/1331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows reflected Cross Site Scripting (XSS). **CVE ID : CVE-2020-8191**		
netscaler_gateway_firmware					
Missing Authorization	7/10/2020	5	Improper access control in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows unauthenticated access to certain URL endpoints. **CVE ID : CVE-2020-8193**	N/A	O-CIT-NETS-100820/1332
Improper Control of Generation of Code ('Code Injection')	7/10/2020	4.3	Reflected code injection in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows the modification of a file download. **CVE ID : CVE-2020-8194**	N/A	O-CIT-NETS-100820/1333
Improper Input Validation	7/10/2020	4	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in limited	N/A	O-CIT-NETS-100820/1334

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure to low privileged users. **CVE ID : CVE-2020-8195**		
Missing Authorization	7/10/2020	4	Improper access control in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in limited information disclosure to low privileged users. **CVE ID : CVE-2020-8196**	N/A	O-CIT-NETS-100820/1335
Improper Privilege Management	7/10/2020	6.5	Privilege escalation vulnerability on Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 allows a low privileged user with management access to execute arbitrary commands. **CVE ID : CVE-2020-8197**	N/A	O-CIT-NETS-100820/1336
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/10/2020	4.3	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in Stored Cross-Site Scripting (XSS). **CVE ID : CVE-2020-8198**	N/A	O-CIT-NETS-100820/1337
Improper Input	7/10/2020	5	Improper input validation in Citrix ADC and Citrix	N/A	O-CIT-NETS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Gateway versions before 11.1-63.9 and 12.0-62.10 allows unauthenticated users to perform a denial of service attack. **CVE ID : CVE-2020-8187**		100820/1338
Improper Preservation of Permissions	7/10/2020	6	Incorrect file permissions in Citrix ADC and Citrix Gateway before versions 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 allows privilege escalation. **CVE ID : CVE-2020-8190**	N/A	O-CIT-NETS-100820/1339
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/10/2020	4.3	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows reflected Cross Site Scripting (XSS). **CVE ID : CVE-2020-8191**	N/A	O-CIT-NETS-100820/1340
sd-wan_wanop					
Missing Authorization	7/10/2020	5	Improper access control in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows unauthenticated access to certain URL endpoints. **CVE ID : CVE-2020-8193**	N/A	O-CIT-SD-W-100820/1341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	7/10/2020	4.3	Reflected code injection in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows the modification of a file download. **CVE ID : CVE-2020-8194**	N/A	O-CIT-SD-W-100820/1342
Improper Input Validation	7/10/2020	4	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in limited information disclosure to low privileged users. **CVE ID : CVE-2020-8195**	N/A	O-CIT-SD-W-100820/1343
Missing Authorization	7/10/2020	4	Improper access control in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in limited information disclosure to low privileged users. **CVE ID : CVE-2020-8196**	N/A	O-CIT-SD-W-100820/1344
Improper Neutralization of Input During	7/10/2020	4.3	Improper input validation in Citrix ADC and Citrix Gateway versions before	N/A	O-CIT-SD-W-100820/1345

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 resulting in Stored Cross-Site Scripting (XSS). **CVE ID : CVE-2020-8198**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/10/2020	4.3	Improper input validation in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows reflected Cross Site Scripting (XSS). **CVE ID : CVE-2020-8191**	N/A	O-CIT-SD-W-100820/1346
Debian					
debian_linux					
Out-of-bounds Read	7/9/2020	2.1	An out-of-bounds read vulnerability was found in the SLiRP networking implementation of the QEMU emulator. This flaw occurs in the icmp6_send_echoreply() routine while replying to an ICMP echo request, also known as ping. This flaw allows a malicious guest to leak the contents of the host memory, resulting in possible information disclosure. This flaw affects versions of libslirp before 4.3.1. **CVE ID : CVE-2020-10756**	N/A	O-DEB-DEBI-100820/1347

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/6/2020	4.3	An issue was discovered in Roundcube Webmail before 1.2.11, 1.3.x before 1.3.14, and 1.4.x before 1.4.7. It allows XSS via a crafted HTML e-mail message, as demonstrated by a JavaScript payload in the xmlns (aka XML namespace) attribute of a HEAD element when an SVG element exists. **CVE ID : CVE-2020-15562**	N/A	O-DEB-DEBI-100820/1348
Improper Input Validation	7/7/2020	4.7	An issue was discovered in Xen through 4.13.x, allowing x86 HVM guest OS users to cause a hypervisor crash. An inverted conditional in x86 HVM guests' dirty video RAM tracking code allows such guests to make Xen de-reference a pointer guaranteed to point at unmapped space. A malicious or buggy HVM guest may cause the hypervisor to crash, resulting in Denial of Service (DoS) affecting the entire host. Xen versions from 4.8 onwards are affected. Xen versions 4.7 and earlier are not affected. Only x86 systems are affected. Arm systems are not affected. Only x86 HVM guests using shadow paging can leverage the vulnerability. In addition, there needs to be an entity	N/A	O-DEB-DEBI-100820/1349

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			actively monitoring a guest's video frame buffer (typically for display purposes) in order for such a guest to be able to leverage the vulnerability. x86 PV guests, as well as x86 HVM guests using hardware assisted paging (HAP), cannot leverage the vulnerability. **CVE ID : CVE-2020-15563**		
Improper Input Validation	7/7/2020	4.9	An issue was discovered in Xen through 4.13.x, allowing Arm guest OS users to cause a hypervisor crash because of a missing alignment check in VCPUOP_register_vcpu_info. The hypercall VCPUOP_register_vcpu_info is used by a guest to register a shared region with the hypervisor. The region will be mapped into Xen address space so it can be directly accessed. On Arm, the region is accessed with instructions that require a specific alignment. Unfortunately, there is no check that the address provided by the guest will be correctly aligned. As a result, a malicious guest could cause a hypervisor crash by passing a misaligned address. A malicious guest administrator may cause a hypervisor crash, resulting	N/A	O-DEB-DEBI-100820/1350

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in a Denial of Service (DoS). All Xen versions are vulnerable. Only Arm systems are vulnerable. x86 systems are not affected. **CVE ID : CVE-2020-15564**		
Uncontrolled Resource Consumption	7/7/2020	6.1	An issue was discovered in Xen through 4.13.x, allowing x86 Intel HVM guest OS users to cause a host OS denial of service or possibly gain privileges because of insufficient cache write-back under VT-d. When page tables are shared between IOMMU and CPU, changes to them require flushing of both TLBs. Furthermore, IOMMUs may be non-coherent, and hence prior to flushing IOMMU TLBs, a CPU cache also needs writing back to memory after changes were made. Such writing back of cached data was missing in particular when splitting large page mappings into smaller granularity ones. A malicious guest may be able to retain read/write DMA access to frames returned to Xen's free pool, and later reused for another purpose. Host crashes (leading to a Denial of Service) and privilege escalation cannot be ruled out. Xen versions	N/A	O-DEB-DEBI-100820/1351

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from at least 3.2 onwards are affected. Only x86 Intel systems are affected. x86 AMD as well as Arm systems are not affected. Only x86 HVM guests using hardware assisted paging (HAP), having a passed through PCI device assigned, and having page table sharing enabled can leverage the vulnerability. Note that page table sharing will be enabled (by default) only if Xen considers IOMMU and CPU large page size support compatible. **CVE ID : CVE-2020-15565**		
Improper Handling of Exceptional Conditions	7/7/2020	4.7	An issue was discovered in Xen through 4.13.x, allowing guest OS users to cause a host OS crash because of incorrect error handling in event-channel port allocation. The allocation of an event-channel port may fail for multiple reasons: (1) port is already in use, (2) the memory allocation failed, or (3) the port we try to allocate is higher than what is supported by the ABI (e.g., 2L or FIFO) used by the guest or the limit set by an administrator (max_event_channels in xl cfg). Due to the missing error checks, only (1) will be considered an error. All	N/A	O-DEB-DEBI-100820/1352

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the other cases will provide a valid port and will result in a crash when trying to access the event channel. When the administrator configured a guest to allow more than 1023 event channels, that guest may be able to crash the host. When Xen is out-of-memory, allocation of new event channels will result in crashing the host rather than reporting an error. Xen versions 4.10 and later are affected. All architectures are affected. The default configuration, when guests are created with xl/libxl, is not vulnerable, because of the default event-channel limit. **CVE ID : CVE-2020-15566**		
Improper Privilege Management	7/7/2020	4.4	An issue was discovered in Xen through 4.13.x, allowing Intel guest OS users to gain privileges or cause a denial of service because of non-atomic modification of a live EPT PTE. When mapping guest EPT (nested paging) tables, Xen would in some circumstances use a series of non-atomic bitfield writes. Depending on the compiler version and optimisation flags, Xen might expose a dangerous partially written PTE to the	N/A	O-DEB-DEBI-100820/1353

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			hardware, which an attacker might be able to race to exploit. A guest administrator or perhaps even an unprivileged guest user might be able to cause denial of service, data corruption, or privilege escalation. Only systems using Intel CPUs are vulnerable. Systems using AMD CPUs, and Arm systems, are not vulnerable. Only systems using nested paging (hap, aka nested paging, aka in this case Intel EPT) are vulnerable. Only HVM and PVH guests can exploit the vulnerability. The presence and scope of the vulnerability depends on the precise optimisations performed by the compiler used to build Xen. If the compiler generates (a) a single 64-bit write, or (b) a series of read-modify-write operations in the same order as the source code, the hypervisor is not vulnerable. For example, in one test build using GCC 8.3 with normal settings, the compiler generated multiple (unlocked) read-modify-write operations in source-code order, which did not constitute a vulnerability. We have not been able to survey		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			compilers; consequently we cannot say which compiler(s) might produce vulnerable code (with which code-generation options). The source code clearly violates the C rules, and thus should be considered vulnerable. **CVE ID : CVE-2020-15567**		
Improper Control of Generation of Code ('Code Injection')	7/2/2020	6.5	The is a code injection vulnerability in versions of Rails prior to 5.0.1 that wouldallow an attacker who controlled the `locals` argument of a `render` call to perform a RCE. **CVE ID : CVE-2020-8163**	N/A	O-DEB-DEBI-100820/1354
Dell					
idrac9_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	7/9/2020	4	Dell EMC iDRAC9 versions prior to 4.20.20.20 contain a Path Traversal Vulnerability. A remote authenticated malicious user with low privileges could potentially exploit this vulnerability by manipulating input parameters to gain unauthorized read access to the arbitrary files. **CVE ID : CVE-2020-5366**	N/A	O-DEL-IDRA-100820/1355
vxrail_d560f_firmware					
Missing Authorization	7/6/2020	5	Dell EMC VxRail versions 4.7.410 and 4.7.411 contain an improper authentication	N/A	O-DEL-VXRA-100820/1356

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. A remote unauthenticated attacker may exploit this vulnerability to obtain sensitive information in an encrypted form. **CVE ID : CVE-2020-5368**		
vxrail_d560_firmware					
Missing Authorization	7/6/2020	5	Dell EMC VxRail versions 4.7.410 and 4.7.411 contain an improper authentication vulnerability. A remote unauthenticated attacker may exploit this vulnerability to obtain sensitive information in an encrypted form. **CVE ID : CVE-2020-5368**	N/A	O-DEL-VXRA-100820/1357
emc_powerscale_onefs					
Incorrect Permission Assignment for Critical Resource	7/6/2020	6.5	Dell EMC Isilon OneFS versions 8.2.2 and earlier and Dell EMC PowerScale version 9.0.0 contain a file permissions vulnerability. An attacker, with network or local file access, could take advantage of insufficiently applied file permissions or gain unauthorized access to files. **CVE ID : CVE-2020-5371**	N/A	O-DEL-EMC_-100820/1358
emc_powerstore_1000_firmware					
Incorrect Authorization	7/6/2020	5	Dell EMC PowerStore versions prior to 1.0.1.0.5.002 contain a vulnerability that exposes	N/A	O-DEL-EMC_-100820/1359

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			test interface ports to external network. A remote unauthenticated attacker could potentially cause Denial of Service via test interface ports which are not used during run time environment. **CVE ID : CVE-2020-5372**		
emc_powerstore_3000_firmware					
Incorrect Authorization	7/6/2020	5	Dell EMC PowerStore versions prior to 1.0.1.0.5.002 contain a vulnerability that exposes test interface ports to external network. A remote unauthenticated attacker could potentially cause Denial of Service via test interface ports which are not used during run time environment. **CVE ID : CVE-2020-5372**	N/A	O-DEL-EMC_-100820/1360
emc_powerstore_5000_firmware					
Incorrect Authorization	7/6/2020	5	Dell EMC PowerStore versions prior to 1.0.1.0.5.002 contain a vulnerability that exposes test interface ports to external network. A remote unauthenticated attacker could potentially cause Denial of Service via test interface ports which are not used during run time environment. **CVE ID : CVE-2020-5372**	N/A	O-DEL-EMC_-100820/1361
emc_powerstore_7000_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	7/6/2020	5	Dell EMC PowerStore versions prior to 1.0.1.0.5.002 contain a vulnerability that exposes test interface ports to external network. A remote unauthenticated attacker could potentially cause Denial of Service via test interface ports which are not used during run time environment. **CVE ID : CVE-2020-5372**	N/A	O-DEL-EMC_-100820/1362
emc_powerstore_9000_firmware					
Incorrect Authorization	7/6/2020	5	Dell EMC PowerStore versions prior to 1.0.1.0.5.002 contain a vulnerability that exposes test interface ports to external network. A remote unauthenticated attacker could potentially cause Denial of Service via test interface ports which are not used during run time environment. **CVE ID : CVE-2020-5372**	N/A	O-DEL-EMC_-100820/1363
powerprotect_x400_firmware					
Files or Directories Accessible to External Parties	7/6/2020	4	Dell PowerProtect Data Manager (PPDM) versions prior to 19.4 and Dell PowerProtect X400 versions prior to 3.2 contain an improper authorization vulnerability. A remote authenticated malicious user may download any file from the affected	N/A	O-DEL-POWE-100820/1364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PowerProtect virtual machines. **CVE ID : CVE-2020-5356**		
Dlink					
dir-610_firmware					
Information Exposure	7/9/2020	5	** UNSUPPORTED WHEN ASSIGNED ** D-Link DIR-610 devices allow Information Disclosure via SERVICES=DEVICE.ACCOUNT%0AAUTHORIZED_GROUP=1 to getcfg.php. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2020-9376**	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10182	O-DLI-DIR--100820/1365
Improper Control of Generation of Code ('Code Injection')	7/9/2020	6.5	** UNSUPPORTED WHEN ASSIGNED ** D-Link DIR-610 devices allow Remote Command Execution via the cmd parameter to command.php. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2020-9377**	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10182	O-DLI-DIR--100820/1366
Fedoraproject					
fedora					
Use of a Broken or Risky Cryptographic Algorithm	7/9/2020	1.2	During RSA key generation, bignum implementations used a variation of the Binary Extended Euclidean Algorithm which entailed significantly input-dependent flow. This	N/A	O-FED-FEDO-100820/1367

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allowed an attacker able to perform electromagnetic-based side channel attacks to record traces leading to the recovery of the secret primes. *Note:* An unmodified Firefox browser does not generate RSA keys in normal operation and is not affected, but products built on top of it might. This vulnerability affects Firefox < 78. **CVE ID : CVE-2020-12402**		
NULL Pointer Dereference	7/7/2020	4	A NULL pointer dereference, or possible use-after-free flaw was found in Samba AD LDAP server in versions before 4.10.17, before 4.11.11 and before 4.12.4. Although some versions of Samba shipped with Red Hat Enterprise Linux do not support Samba in AD mode, the affected code is shipped with the libldb package. This flaw allows an authenticated user to possibly trigger a use-after-free or NULL pointer dereference. The highest threat from this vulnerability is to system availability. **CVE ID : CVE-2020-10730**	N/A	O-FED-FEDO-100820/1368
Uncontrolled Resource Consumption	7/7/2020	7.8	A flaw was found in all Samba versions before 4.10.17, before 4.11.11 and	N/A	O-FED-FEDO-100820/1369

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 4.12.4 in the way it processed NetBios over TCP/IP. This flaw allows a remote attacker could to cause the Samba server to consume excessive CPU use, resulting in a denial of service. This highest threat from this vulnerability is to system availability. **CVE ID : CVE-2020-10745**		
Use After Free	7/6/2020	4	A use-after-free flaw was found in all samba LDAP server versions before 4.10.17, before 4.11.11, before 4.12.4 used in a AC DC configuration. A Samba LDAP user could use this flaw to crash samba. **CVE ID : CVE-2020-10760**	N/A	O-FED-FEDO-100820/1370
Improper Input Validation	7/14/2020	7.5	The bubblewrap sandbox of WebKitGTK and WPE WebKit, prior to 2.28.3, failed to properly block access to CLONE_NEWUSER and the TIOCSTI ioctl. CLONE_NEWUSER could potentially be used to confuse xdg-desktop-portal, which allows access outside the sandbox. TIOCSTI can be used to directly execute commands outside the sandbox by writing to the controlling terminal's input buffer, similar to CVE-2017-5226.	https://www.openwall.com/lists/oss-security/2020/07/10/1	O-FED-FEDO-100820/1371

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-13753		
Improper Input Validation	7/6/2020	5	A flaw was found in the AD DC NBT server in all Samba versions before 4.10.17, before 4.11.11 and before 4.12.4. A samba user could send an empty UDP packet to cause the samba server to crash. **CVE ID : CVE-2020-14303**	https://security.netapp.com/advisory/ntap-20200709-0003/	O-FED-FEDO-100820/1372
Improper Input Validation	7/2/2020	5	LibRaw before 0.20-RC1 lacks a thumbnail size range check. This affects decoders/unpack_thumb.cpp, postprocessing/mem_image.cpp, and utils/thumb_utils.cpp. For example, malloc(sizeof(libraw_processed_image_t)+T.tlength) occurs without validating T.tlength. **CVE ID : CVE-2020-15503**	N/A	O-FED-FEDO-100820/1373
Freebsd					
freebsd					
Use After Free	7/9/2020	6.8	In FreeBSD 12.1-STABLE before r359565, 12.1-RELEASE before p7, 11.4-STABLE before r362975, 11.4-RELEASE before p1, and 11.3-RELEASE before p11, missing synchronization in the IPV6_2292PKTOPTIONS socket option set handler contained a race condition allowing a malicious application to modify	https://security.netapp.com/advisory/ntap-20200724-0002/	O-FRE-FREE-100820/1374

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory after being freed, possibly resulting in code execution. **CVE ID : CVE-2020-7457**		
Out-of-bounds Write	7/9/2020	7.5	In FreeBSD 12.1-STABLE before r362281, 11.4-STABLE before r362281, and 11.4-RELEASE before p1, long values in the user-controlled PATH environment variable cause posix_spawnp to write beyond the end of the heap allocated stack possibly leading to arbitrary code execution. **CVE ID : CVE-2020-7458**	https://security.netapp.com/advisory/ntap-20200724-0002/	O-FRE-FREE-100820/1375
Geovision					
gv-as210_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/8/2020	7.5	Buffer overflow exists in Geovision Door Access Control device family, an unauthenticated remote attacker can execute arbitrary command. **CVE ID : CVE-2020-3931**	https://www.acronis.com/en-us/blog/posts/backdoor-wide-open-critical-vulnerabilities-uncovered-geovision, https://www.twcert.org.tw/tw/cp-132-3754-b77d0-1.html	O-GEO-GV-A-100820/1376
gv-as410_firmware					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/8/2020	7.5	Buffer overflow exists in Geovision Door Access Control device family, an unauthenticated remote attacker can execute arbitrary command. **CVE ID : CVE-2020-3931**	https://www.acronis.com/en-us/blog/posts/backdoor-wide-open-critical-vulnerabilities-uncovered-geovision, https://www.twcert.org.tw/tw/cp-132-3754-b77d0-1.html	O-GEO-GV-A-100820/1377
gv-as810_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/8/2020	7.5	Buffer overflow exists in Geovision Door Access Control device family, an unauthenticated remote attacker can execute arbitrary command. **CVE ID : CVE-2020-3931**	https://www.acronis.com/en-us/blog/posts/backdoor-wide-open-critical-vulnerabilities-uncovered-geovision, https://www.twcert.org.tw/tw/cp-132-3754-b77d0-1.html	O-GEO-GV-A-100820/1378
gv-gf1921_firmware					
Buffer Copy without	7/8/2020	7.5	Buffer overflow exists in Geovision Door Access	https://www.acronis.c	O-GEO-GV-G-100820/1379

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			Control device family, an unauthenticated remote attacker can execute arbitrary command. **CVE ID : CVE-2020-3931**	om/en-us/blog/posts/backdoor-wide-open-critical-vulnerabilities-uncovered-geovision, https://www.twcert.org.tw/tw/cp-132-3754-b77d0-1.html	
gv-as1010_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/8/2020	7.5	Buffer overflow exists in Geovision Door Access Control device family, an unauthenticated remote attacker can execute arbitrary command. **CVE ID : CVE-2020-3931**	https://www.acronis.com/en-us/blog/posts/backdoor-wide-open-critical-vulnerabilities-uncovered-geovision, https://www.twcert.org.tw/tw/cp-132-3754-b77d0-1.html	O-GEO-GV-A-100820/1380
gv-gf1922_firmware					
Buffer Copy without Checking Size of Input	7/8/2020	7.5	Buffer overflow exists in Geovision Door Access Control device family, an unauthenticated remote	https://www.acronis.com/en-us/blog/po	O-GEO-GV-G-100820/1381

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			attacker can execute arbitrary command. **CVE ID : CVE-2020-3931**	sts/backdoor-wide-open-critical-vulnerabilities-uncovered-geovision, https://www.twcert.org.tw/tw/cp-132-3754-b77d0-1.html	
Google					
android					
N/A	7/7/2020	2.1	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) software. Cameralyzer allows attackers to write files to the SD card. The Samsung ID is SVE-2020-16830 (July 2020). **CVE ID : CVE-2020-15577**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-100820/1382
Incorrect Default Permissions	7/7/2020	2.1	An issue was discovered on Samsung mobile devices with O(8.x) software. FactoryCamera does not properly restrict runtime permissions. The Samsung ID is SVE-2020-17270 (July 2020). **CVE ID : CVE-2020-15578**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-100820/1383
N/A	7/7/2020	5	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software.	https://security.samsungmobile.com/security	O-GOO-ANDR-100820/1384

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Attackers can bypass Factory Reset Protection (FRP) via the KNOX API. The Samsung ID is SVE-2020-17318 (July 2020). **CVE ID : CVE-2020-15579**	Update.smsb	
N/A	7/7/2020	2.1	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. Attackers can bypass Factory Reset Protection (FRP) by enrolling a new lock password. The Samsung ID is SVE-2020-17328 (July 2020). **CVE ID : CVE-2020-15580**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-100820/1385
Information Exposure	7/7/2020	5	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. The kernel logging feature allows attackers to discover virtual addresses via vectors involving shared memory. The Samsung ID is SVE-2020-17605 (July 2020). **CVE ID : CVE-2020-15581**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-100820/1386
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/7/2020	4.3	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) (Exynos 7885 chipsets) software. The Bluetooth Low Energy (BLE) component has a buffer overflow with a resultant deadlock or crash. The Samsung ID is	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-100820/1387

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SVE-2020-16870 (July 2020). **CVE ID : CVE-2020-15582**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	7/7/2020	2.1	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. StickerProvider allows directory traversal for access to system files. The Samsung ID is SVE-2020-17665 (July 2020). **CVE ID : CVE-2020-15583**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-100820/1388
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/7/2020	7.1	An issue was discovered on Samsung mobile devices with Q(10.0) software. Attackers can trigger an out-of-bounds access and device reset via a 4K wallpaper image because ImageProcessHelper mishandles boundary checks. The Samsung ID is SVE-2020-18056 (July 2020). **CVE ID : CVE-2020-15584**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-100820/1389
gpononu					
1ge_router_wifi_onu_v2801rw_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	7/15/2020	9	Guangzhou 1GE ONU V2801RW 1.9.1-181203 through 2.9.0-181024 and V2804RGW 1.9.1-181203 through 2.9.0-181024 devices allow remote attackers to execute arbitrary OS commands via shell metacharacters in the boaform/admin/formPing	N/A	O-GPO-1GE_-100820/1390

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Dest IP Address field. **CVE ID : CVE-2020-8958**		
1ge\+3fe\+wifi_onu_v2804rgw_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	7/15/2020	9	Guangzhou 1GE ONU V2801RW 1.9.1-181203 through 2.9.0-181024 and V2804RGW 1.9.1-181203 through 2.9.0-181024 devices allow remote attackers to execute arbitrary OS commands via shell metacharacters in the boaform/admin/formPing Dest IP Address field. **CVE ID : CVE-2020-8958**	N/A	O-GPO-1GE\-100820/1391
Huawei					
mate_30_pro_firmware					
Improper Authentication	7/6/2020	1.9	HUAWEI Mate 30 Pro with versions earlier than 10.1.0.150(C00E136R5P3) have is an improper authentication vulnerability. The device does not sufficiently validate certain credential of user's face, an attacker could craft the credential of the user, successful exploit could allow the attacker to pass the authentication with the crafted credential. **CVE ID : CVE-2020-1838**	N/A	O-HUA-MATE-100820/1392
changxiang_8_plus_firmware					
Improper Input Validation	7/6/2020	2.9	ChangXiang 8 Plus with versions earlier than 9.1.0.136(C00E121R1P6T8) have a denial of service	N/A	O-HUA-CHAN-100820/1393

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. The device does not properly handle certain message from base station, the attacker could craft a fake base station to launch the attack. Successful exploit could cause a denial of signal service condition. **CVE ID : CVE-2020-1837**		
p30_pro_firmware					
Information Exposure	7/6/2020	2.9	HUAWEI P30 with versions earlier than 10.1.0.160(C00E160R2P11) and HUAWEI P30 Pro with versions earlier than 10.1.0.160(C00E160R2P8) have an information disclosure vulnerability. Certain function's default configuration in the system seems insecure, an attacker should craft a WI-FI hotspot to launch the attack. Successful exploit could cause information disclosure. **CVE ID : CVE-2020-1836**	N/A	O-HUA-P30_-100820/1394
Information Exposure	7/10/2020	3.3	HUAWEI P30 and HUAWEI P30 Pro smartphones with versions earlier than 10.1.0.123(C432E22R2P5) and versions earlier than 10.1.0.160(C00E160R2P8) have an information disclosure vulnerability. Certain WI-FI function's default configuration in the system seems insecure, an attacker should craft a WI-	N/A	O-HUA-P30_-100820/1395

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FI hotspot to launch the attack. Successful exploit could cause information disclosure. **CVE ID : CVE-2020-9260**		
p30_firmware					
Information Exposure	7/6/2020	2.9	HUAWEI P30 with versions earlier than 10.1.0.160(C00E160R2P11) and HUAWEI P30 Pro with versions earlier than 10.1.0.160(C00E160R2P8) have an information disclosure vulnerability. Certain function's default configuration in the system seems insecure, an attacker should craft a WI-FI hotspot to launch the attack. Successful exploit could cause information disclosure. **CVE ID : CVE-2020-1836**	N/A	O-HUA-P30_-100820/1396
Improper Verification of Cryptographic Signature	7/6/2020	4.3	HUAWEI P30 with versions earlier than 10.1.0.135(C00E135R2P11) have an improper signature verification vulnerability. The system does not improper check signature of specific software package, an attacker may exploit this vulnerability to load a crafted software package to the device. **CVE ID : CVE-2020-9226**	N/A	O-HUA-P30_-100820/1397
Information Exposure	7/10/2020	1.9	HUAWEI P30 smartphone with versions earlier than	N/A	O-HUA-P30_-100820/1398

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.1.0.135(C00E135R2P11) have an improper input verification vulnerability. An attribution in a module is not set correctly and some verification is lacked. Attackers with local access can exploit this vulnerability by injecting malicious fragment. This may lead to user information leak. **CVE ID : CVE-2020-9258**		
Information Exposure	7/10/2020	3.3	HUAWEI P30 and HUAWEI P30 Pro smartphones with versions earlier than 10.1.0.123(C432E22R2P5) and versions earlier than 10.1.0.160(C00E160R2P8) have an information disclosure vulnerability. Certain WI-FI function's default configuration in the system seems insecure, an attacker should craft a WI-FI hotspot to launch the attack. Successful exploit could cause information disclosure. **CVE ID : CVE-2020-9260**	N/A	O-HUA-P30_-100820/1399
mate_30_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	7/6/2020	3.7	HUAWEI Mate 30 with versions earlier than 10.1.0.150(C00E136R5P3) have a race condition vulnerability. There is a timing window exists in which certain pointer members can be modified by another process that is	N/A	O-HUA-MATE-100820/1400

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating concurrently, an attacker should trick the user into running a crafted application with high privilege, successful exploit could cause code execution. **CVE ID : CVE-2020-1839**		
Access of Resource Using Incompatible Type ('Type Confusion')	7/6/2020	6.8	HUAWEI Mate 30 with versions earlier than 10.1.0.150(C00E136R5P3) have a type confusion vulnerability. The system does not properly check and transform the type of certain variable, the attacker tricks the user into installing then running a crafted application, successful exploit could cause code execution. **CVE ID : CVE-2020-9261**	N/A	O-HUA-MATE-100820/1401
Use After Free	7/6/2020	6.8	HUAWEI Mate 30 with versions earlier than 10.1.0.150(C00E136R5P3) have a use after free vulnerability. There is a condition exists that the system would reference memory after it has been freed, the attacker should trick the user into running a crafted application with high privilege, successful exploit could cause code execution. **CVE ID : CVE-2020-9262**	N/A	O-HUA-MATE-100820/1402
Linux					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
linux_kernel					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	7/8/2020	6.5	The VeloCloud Orchestrator does not apply correct input validation which allows for blind SQL-injection. A malicious actor with tenant access to Velocloud Orchestrator could enter specially crafted SQL queries and obtain data to which they are not privileged. **CVE ID : CVE-2020-3973**	N/A	O-LIN-LINU-100820/1403
N/A	7/9/2020	4.3	IBM Guardium Activity Insights 10.6 and 11.0 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 174682. **CVE ID : CVE-2020-4173**	https://www.ibm.com/support/pages/node/6244924	O-LIN-LINU-100820/1404
Out-of-bounds Read	7/1/2020	5	In nDPI through 3.2, the Oracle protocol dissector has a heap-based buffer over-read in ndpi_search_oracle in lib/protocols/oracle.c. **CVE ID : CVE-2020-15476**	N/A	O-LIN-LINU-100820/1405
Incorrect	7/15/2020	7.2	An issue was discovered in	N/A	O-LIN-LINU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authorization			drivers/acpi/acpi_configfs.c in the Linux kernel before 5.7.7. Injection of malicious ACPI tables via configfs could be used by attackers to bypass lockdown and secure boot restrictions, aka CID-75b0cea7bf30. **CVE ID : CVE-2020-15780**		100820/1406
Uncontrolled Resource Consumption	7/1/2020	5	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 is vulnerable to a denial of service, caused by improper handling of Secure Sockets Layer (SSL) renegotiation requests. By sending specially-crafted requests, a remote attacker could exploit this vulnerability to increase the resource usage on the system. IBM X-Force ID: 178507. **CVE ID : CVE-2020-4355**	https://www.ibm.com/support/pages/node/6242350	O-LIN-LINU-100820/1407
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/1/2020	7.2	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 is vulnerable to a buffer overflow, caused by improper bounds checking which could allow a local attacker to execute arbitrary code on the system with root privileges. IBM X-Force ID: 178960.	https://www.ibm.com/support/pages/node/6242332	O-LIN-LINU-100820/1408

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		🟧	**CVE ID : CVE-2020-4363**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	7/1/2020	1.9	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a local user to obtain sensitive information using a race condition of a symbolic link. IBM X-Force ID: 179268. **CVE ID : CVE-2020-4386**	https://www.ibm.com/support/pages/node/6242342	O-LIN-LINU-100820/1409
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	7/1/2020	1.9	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a local user to obtain sensitive information using a race condition of a symbolic link. IBM X-Force ID: 179269. **CVE ID : CVE-2020-4387**	https://www.ibm.com/support/pages/node/6242336	O-LIN-LINU-100820/1410
Incorrect Permission Assignment for Critical Resource	7/1/2020	3.6	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a local attacker to perform unauthorized actions on the system, caused by improper usage of shared memory. By sending a specially-crafted request, an attacker could exploit this vulnerability to obtain sensitive information or cause a denial of service. IBM X-Force ID: 179989.	https://www.ibm.com/support/pages/node/6242356	O-LIN-LINU-100820/1411

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-4414		
Improper Resource Shutdown or Release	7/1/2020	5	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow an unauthenticated attacker to cause a denial of service due a hang in the execution of a terminate command. IBM X-Force ID: 180076. **CVE ID : CVE-2020-4420**	https://www.ibm.com/support/pages/node/6242362	O-LIN-LINU-100820/1412
Information Exposure Through Log Files	7/8/2020	5	A sensitive information disclosure vulnerability in Tableau Server 10.5, 2018.x, 2019.x, 2020.x released before June 26, 2020, could allow access to sensitive information in log files. **CVE ID : CVE-2020-6938**	N/A	O-LIN-LINU-100820/1413
Microsoft					
windows					
Uncontrolled Search Path Element	7/9/2020	6.9	When the Windows DLL "webauthn.dll" was missing from the Operating System, and a malicious one was placed in a folder in the user's %PATH%, Firefox may have loaded the DLL, leading to arbitrary code execution. *Note: This issue only affects the Windows operating system; other operating systems are unaffected.* This vulnerability affects Firefox < 78.	N/A	O-MIC-WIND-100820/1414

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-12423		
Untrusted Search Path	7/15/2020	6.9	An untrusted search path remote code execution (RCE) vulnerability in the Trend Micro Secuity 2020 (v16.0.0.1146 and below) consumer family of products could allow an attacker to run arbitrary code on a vulnerable system. As the Trend Micro installer tries to load DLL files from its current directory, an arbitrary DLL could also be loaded with the same privileges as the installer if run as Administrator. User interaction is required to exploit the vulnerbaility in that the target must open a malicious directory or device. **CVE ID : CVE-2020-15602**	N/A	O-MIC-WIND-100820/1415
Out-of-bounds Read	7/15/2020	7.8	An invalid memory read vulnerability in a Trend Micro Secuity 2020 (v16.0.0.1302 and below) consumer family of products' driver could allow an attacker to manipulate the specific driver to do a system call operation with an invalid address, resulting in a potential system crash. **CVE ID : CVE-2020-15603**	N/A	O-MIC-WIND-100820/1416
Uncontrolled Resource	7/1/2020	5	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7,	https://www.ibm.com/support/pa	O-MIC-WIND-100820/1417

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Consumption			10.1, 10.5, 11.1, and 11.5 is vulnerable to a denial of service, caused by improper handling of Secure Sockets Layer (SSL) renegotiation requests. By sending specially-crafted requests, a remote attacker could exploit this vulnerability to increase the resource usage on the system. IBM X-Force ID: 178507. **CVE ID : CVE-2020-4355**	ges/node/6242350	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/1/2020	7.2	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 is vulnerable to a buffer overflow, caused by improper bounds checking which could allow a local attacker to execute arbitrary code on the system with root privileges. IBM X-Force ID: 178960. **CVE ID : CVE-2020-4363**	https://www.ibm.com/support/pages/node/6242332	O-MIC-WIND-100820/1418
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	7/1/2020	1.9	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a local user to obtain sensitive information using a race condition of a symbolic link. IBM X-Force ID: 179268. **CVE ID : CVE-2020-4386**	https://www.ibm.com/support/pages/node/6242342	O-MIC-WIND-100820/1419

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	7/1/2020	1.9	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a local user to obtain sensitive information using a race condition of a symbolic link. IBM X-Force ID: 179269. **CVE ID : CVE-2020-4387**	https://www.ibm.com/support/pages/node/6242336	O-MIC-WIND-100820/1420
Incorrect Permission Assignment for Critical Resource	7/1/2020	3.6	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a local attacker to perform unauthorized actions on the system, caused by improper usage of shared memory. By sending a specially-crafted request, an attacker could exploit this vulnerability to obtain sensitive information or cause a denial of service. IBM X-Force ID: 179989. **CVE ID : CVE-2020-4414**	https://www.ibm.com/support/pages/node/6242356	O-MIC-WIND-100820/1421
Improper Resource Shutdown or Release	7/1/2020	5	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow an unauthenticated attacker to cause a denial of service due a hang in the execution of a terminate command. IBM X-Force ID: 180076. **CVE ID : CVE-2020-4420**	https://www.ibm.com/support/pages/node/6242362	O-MIC-WIND-100820/1422

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure Through Log Files	7/8/2020	5	A sensitive information disclosure vulnerability in Tableau Server 10.5, 2018.x, 2019.x, 2020.x released before June 26, 2020, could allow access to sensitive information in log files. **CVE ID : CVE-2020-6938**	N/A	O-MIC-WIND-100820/1423
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/8/2020	4.3	A security vulnerability in HPE IceWall SSO Dfw and Dgfw (Domain Gateway Option) could be exploited remotely to cause a remote cross-site scripting (XSS). HPE has provided the following information to resolve this vulnerability in HPE IceWall SSO DFW and Dgfw: https://www.hpe.com/jp/icewall_patchaccess **CVE ID : CVE-2020-7140**	N/A	O-MIC-WIND-100820/1424
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	7/10/2020	7.5	RAONWIZ v2018.0.2.50 and eariler versions contains a vulnerability that could allow remote files to be downloaded and excuted by lack of validation to file extension, witch can used as remote-code-excution attacks by hackers File download & execution vulnerability in ___COMPONENT___ of RAONWIZ RAON KUpload allows ___ATTACKER/ATTACK___ to cause ___IMPACT___. This issue affects:	N/A	O-MIC-WIND-100820/1425

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			RAONWIZ RAON KUpload 2018.0.2.50 versions prior to 2018.0.2.51 on Windows. **CVE ID : CVE-2020-7814**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	7/10/2020	7.5	XPLATFORM v9.2.260 and eariler versions contain a vulnerability that could allow remote files to be downloaded by setting the arguments to the vulnerable method. this can be leveraged for code execution. File download vulnerability in ___COMPONENT___ of TOBESOFT XPLATFORM allows ___ATTACKER/ATTACK___ to cause ___IMPACT___. This issue affects: TOBESOFT XPLATFORM 9.2.250 versions prior to 9.2.260 on Windows. **CVE ID : CVE-2020-7815**	N/A	O-MIC-WIND-100820/1426
Improper Input Validation	7/2/2020	7.5	Nexacro14/17 ExtCommonApiV13 Library under 2019.9.6 version contain a vulnerability that could allow remote attacker to execute arbitrary code by setting the arguments to the vulnerable API. This can be leveraged for code execution by rebooting the victim's PC **CVE ID : CVE-2020-7820**	http://support.tobesoft.co.kr/Support/index.html, https://www.krcert.or.kr/krcert/secNoticeView.do?bulletin_writing_sequence=35491	O-MIC-WIND-100820/1427
Improper Input	7/2/2020	7.5	Nexacro14/17	http://supp	O-MIC-WIND-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			ExtCommonApiV13 Library under 2019.9.6 version contain a vulnerability that could allow remote attacker to execute arbitrary code by modifying the value of registry path. This can be leveraged for code execution by rebooting the victim's PC **CVE ID : CVE-2020-7821**	ort.tobesoft.co.kr/Support/index.html, https://www.krcert.or.kr/krcert/secNoticeView.do?bulletin_writing_sequence=35491	100820/1428
windows_10					
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1085**	N/A	O-MIC-WIND-100820/1429
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1427, CVE-2020-1428, CVE-2020-1438. **CVE ID : CVE-2020-1390**	N/A	O-MIC-WIND-100820/1430
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists when	N/A	O-MIC-WIND-100820/1431

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the Windows Agent Activation Runtime (AarSvc) fails to properly handle objects in memory, aka 'Windows Agent Activation Runtime Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1391**		
N/A	7/14/2020	6.8	A remote code execution vulnerability exists in .NET Framework, Microsoft SharePoint, and Visual Studio when the software fails to check the source markup of XML file input, aka '.NET Framework, SharePoint Server, and Visual Studio Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1147**	N/A	O-MIC-WIND-100820/1432
Improper Privilege Management	7/14/2020	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-2020-1353, CVE-2020-1370, CVE-2020-1399, CVE-2020-1404, CVE-2020-1413, CVE-2020-1414, CVE-2020-1415, CVE-2020-1422. **CVE ID : CVE-2020-1249**	N/A	O-MIC-WIND-100820/1433
Improper Input Validation	7/14/2020	4	This security update corrects a denial of service in the Local Security	N/A	O-MIC-WIND-100820/1434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Authority Subsystem Service (LSASS) caused when an authenticated attacker sends a specially crafted authentication request, aka 'Local Security Authority Subsystem Service Denial of Service Vulnerability'. **CVE ID : CVE-2020-1267**		
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists when Windows Mobile Device Management (MDM) Diagnostics improperly handles junctions, aka 'Windows Mobile Device Management Diagnostics Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1330**	N/A	O-MIC-WIND-100820/1435
Improper Privilege Management	7/14/2020	3.7	An elevation of privilege vulnerability exists when Group Policy Services Policy Processing improperly handle reparse points, aka 'Group Policy Services Policy Processing Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1333**	N/A	O-MIC-WIND-100820/1436
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from	N/A	O-MIC-WIND-100820/1437

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-1411. **CVE ID : CVE-2020-1336**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows WalletService handles objects in memory, aka 'Windows WalletService Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1362, CVE-2020-1369. **CVE ID : CVE-2020-1344**	N/A	O-MIC-WIND-100820/1438
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Modules Installer improperly handles file operations, aka 'Windows Modules Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1346**	N/A	O-MIC-WIND-100820/1439
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Storage Services improperly handle file operations, aka 'Windows Storage Services Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1347**	N/A	O-MIC-WIND-100820/1440
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists when the Windows Graphics component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure	N/A	O-MIC-WIND-100820/1441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. **CVE ID : CVE-2020-1351**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows USO Core Worker improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows USO Core Worker Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1352**	N/A	O-MIC-WIND-100820/1442
Improper Privilege Management	7/14/2020	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-2020-1249, CVE-2020-1370, CVE-2020-1399, CVE-2020-1404, CVE-2020-1413, CVE-2020-1414, CVE-2020-1415, CVE-2020-1422. **CVE ID : CVE-2020-1353**	N/A	O-MIC-WIND-100820/1443
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows	N/A	O-MIC-WIND-100820/1444

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UPnP Device Host Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1430. **CVE ID : CVE-2020-1354**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	4.6	A remote code execution vulnerability exists when the Windows Font Driver Host improperly handles memory.An attacker who successfully exploited the vulnerability would gain execution on a victim system.The security update addresses the vulnerability by correcting how the Windows Font Driver Host handles memory., aka 'Windows Font Driver Host Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1355**	N/A	O-MIC-WIND-100820/1445
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows System Events Broker improperly handles file operations, aka 'Windows System Events Broker Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1357**	N/A	O-MIC-WIND-100820/1446
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists when the Windows Resource Policy component improperly handles memory.To exploit this	N/A	O-MIC-WIND-100820/1447

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Resource Policy Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1358**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Cryptography Next Generation (CNG) Key Isolation service improperly handles memory, aka 'Windows CNG Key Isolation Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1384. **CVE ID : CVE-2020-1359**	N/A	O-MIC-WIND-100820/1448
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Profile Service improperly handles file operations, aka 'Windows Profile Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1360**	N/A	O-MIC-WIND-100820/1449
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists in the way that the WalletService handles memory.To exploit the vulnerability, an attacker would first need code execution on a victim system, aka 'Windows	N/A	O-MIC-WIND-100820/1450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WalletService Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1361**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows WalletService handles objects in memory, aka 'Windows WalletService Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1344, CVE-2020-1369. **CVE ID : CVE-2020-1362**	N/A	O-MIC-WIND-100820/1451
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Picker Platform improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Picker Platform Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1363**	N/A	O-MIC-WIND-100820/1452
Improper Input Validation	7/14/2020	3.6	A denial of service vulnerability exists in the way that the WalletService handles files, aka 'Windows WalletService Denial of Service Vulnerability'. **CVE ID : CVE-2020-1364**	N/A	O-MIC-WIND-100820/1453
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Event Logging Service	N/A	O-MIC-WIND-100820/1454

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Event Logging Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1371. **CVE ID : CVE-2020-1365**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Print Workflow Service improperly handles objects in memory, aka 'Windows Print Workflow Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1366**	N/A	O-MIC-WIND-100820/1455
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1389, CVE-2020-1419, CVE-2020-1426. **CVE ID : CVE-2020-1367**	N/A	O-MIC-WIND-100820/1456
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Credential Enrollment Manager service handles objects in	N/A	O-MIC-WIND-100820/1457

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory, aka 'Windows Credential Enrollment Manager Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1368**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows WalletService handles objects in memory, aka 'Windows WalletService Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1344, CVE-2020-1362. **CVE ID : CVE-2020-1369**	N/A	O-MIC-WIND-100820/1458
Improper Privilege Management	7/14/2020	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-2020-1249, CVE-2020-1353, CVE-2020-1399, CVE-2020-1404, CVE-2020-1413, CVE-2020-1414, CVE-2020-1415, CVE-2020-1422. **CVE ID : CVE-2020-1370**	N/A	O-MIC-WIND-100820/1459
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Event Logging Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain	N/A	O-MIC-WIND-100820/1460

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution on the victim system, aka 'Windows Event Logging Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1365. **CVE ID : CVE-2020-1371**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when Windows Mobile Device Management (MDM) Diagnostics improperly handles objects in memory, aka 'Windows Mobile Device Management Diagnostics Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1405. **CVE ID : CVE-2020-1372**	N/A	O-MIC-WIND-100820/1461
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1390, CVE-2020-1427, CVE-2020-1428, CVE-2020-1438. **CVE ID : CVE-2020-1373**	N/A	O-MIC-WIND-100820/1462
Improper Restriction of Operations	7/14/2020	5.1	A remote code execution vulnerability exists in the Windows Remote Desktop	N/A	O-MIC-WIND-100820/1463

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1374**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when Windows improperly handles COM object creation, aka 'Windows COM Server Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1375**	N/A	O-MIC-WIND-100820/1464
Use After Free	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1382. **CVE ID : CVE-2020-1381**	N/A	O-MIC-WIND-100820/1465
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1381. **CVE ID : CVE-2020-1382**	N/A	O-MIC-WIND-100820/1466

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Cryptography Next Generation (CNG) Key Isolation service improperly handles memory, aka 'Windows CNG Key Isolation Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1359. **CVE ID : CVE-2020-1384**	N/A	O-MIC-WIND-100820/1467
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Credential Picker handles objects in memory, aka 'Windows Credential Picker Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1385**	N/A	O-MIC-WIND-100820/1468
Information Exposure	7/14/2020	2.1	An information vulnerability exists when Windows Connected User Experiences and Telemetry Service improperly discloses file information, aka 'Connected User Experiences and Telemetry Service Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1386**	N/A	O-MIC-WIND-100820/1469
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way the Windows Push Notification Service handles objects in	N/A	O-MIC-WIND-100820/1470

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory, aka 'Windows Push Notification Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1387**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the psmsrv.dll handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1392, CVE-2020-1394, CVE-2020-1395. **CVE ID : CVE-2020-1388**	N/A	O-MIC-WIND-100820/1471
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1367, CVE-2020-1419, CVE-2020-1426. **CVE ID : CVE-2020-1389**	N/A	O-MIC-WIND-100820/1472
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Delivery Optimization service improperly handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1388, CVE-2020-1394, CVE-2020-1395.	N/A	O-MIC-WIND-100820/1473

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1392		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Diagnostics Hub Standard Collector Service fails to properly sanitize input, leading to an unsecure library-loading behavior, aka 'Windows Diagnostics Hub Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1418. **CVE ID : CVE-2020-1393**	N/A	O-MIC-WIND-100820/1474
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Geolocation Framework handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1388, CVE-2020-1392, CVE-2020-1395. **CVE ID : CVE-2020-1394**	N/A	O-MIC-WIND-100820/1475
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Speech Brokered API handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1388, CVE-2020-1392, CVE-2020-1394. **CVE ID : CVE-2020-1395**	N/A	O-MIC-WIND-100820/1476

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to Advanced Local Procedure Call (ALPC).An attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the local system, aka 'Windows ALPC Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1396**	N/A	O-MIC-WIND-100820/1477
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists in Windows when the Windows Imaging Component fails to properly handle objects in memory, aka 'Windows Imaging Component Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1397**	N/A	O-MIC-WIND-100820/1478
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when Windows Lockscreen fails to properly handle Ease of Access dialog.An attacker who successfully exploited the vulnerability could execute commands with elevated permissions.The security update addresses the vulnerability by ensuring that the Ease of Access dialog is handled properly., aka 'Windows Lockscreen Elevation of	N/A	O-MIC-WIND-100820/1479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability'. **CVE ID : CVE-2020-1398**		
Improper Privilege Management	7/14/2020	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-2020-1249, CVE-2020-1353, CVE-2020-1370, CVE-2020-1404, CVE-2020-1413, CVE-2020-1414, CVE-2020-1415, CVE-2020-1422. **CVE ID : CVE-2020-1399**	N/A	O-MIC-WIND-100820/1480
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	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-2020-1401, CVE-2020-1407. **CVE ID : CVE-2020-1400**	N/A	O-MIC-WIND-100820/1481
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	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-2020-1400, CVE-2020-1407. **CVE ID : CVE-2020-1401**	N/A	O-MIC-WIND-100820/1482

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	7/14/2020	7.2	An elevation of privilege vulnerability exists when the Windows ActiveX Installer Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows ActiveX Installer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1402**	N/A	O-MIC-WIND-100820/1483
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	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'. **CVE ID : CVE-2020-1403**	N/A	O-MIC-WIND-100820/1484
Improper Privilege Management	7/14/2020	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-2020-1249, CVE-2020-1353, CVE-2020-1370, CVE-2020-1399, CVE-2020-1413, CVE-2020-1414, CVE-2020-1415, CVE-2020-1422. **CVE ID : CVE-2020-1404**	N/A	O-MIC-WIND-100820/1485
Improper Privilege	7/14/2020	3.6	An elevation of privilege vulnerability exists when	N/A	O-MIC-WIND-100820/1486

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Windows Mobile Device Management (MDM) Diagnostics improperly handles junctions, aka 'Windows Mobile Device Management Diagnostics Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1372. **CVE ID : CVE-2020-1405**		
Improper Privilege Management	7/14/2020	7.2	An elevation of privilege vulnerability exists in the way that the Windows Network List Service handles objects in memory, aka 'Windows Network List Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1406**	N/A	O-MIC-WIND-100820/1487
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	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-2020-1400, CVE-2020-1401. **CVE ID : CVE-2020-1407**	N/A	O-MIC-WIND-100820/1488
Origin Validation Error	7/14/2020	9.3	A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Microsoft Graphics	N/A	O-MIC-WIND-100820/1489

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1408**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	9.3	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1409**	N/A	O-MIC-WIND-100820/1490
N/A	7/14/2020	9.3	A remote code execution vulnerability exists when Windows Address Book (WAB) improperly processes vcard files.To exploit the vulnerability, an attacker could send a malicious vcard that a victim opens using Windows Address Book (WAB), aka 'Windows Address Book Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1410**	N/A	O-MIC-WIND-100820/1491
Improper Privilege Management	7/14/2020	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-2020-1336. **CVE ID : CVE-2020-1411**	N/A	O-MIC-WIND-100820/1492
Improper Restriction of Operations	7/14/2020	9.3	A remote code execution vulnerability exists in the way that Microsoft	N/A	O-MIC-WIND-100820/1493

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1412**		
Improper Privilege Management	7/14/2020	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-2020-1249, CVE-2020-1353, CVE-2020-1370, CVE-2020-1399, CVE-2020-1404, CVE-2020-1414, CVE-2020-1415, CVE-2020-1422. **CVE ID : CVE-2020-1413**	N/A	O-MIC-WIND-100820/1494
Improper Privilege Management	7/14/2020	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-2020-1249, CVE-2020-1353, CVE-2020-1370, CVE-2020-1399, CVE-2020-1404, CVE-2020-1413, CVE-2020-1415, CVE-2020-1422. **CVE ID : CVE-2020-1414**	N/A	O-MIC-WIND-100820/1495
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Runtime	N/A	O-MIC-WIND-100820/1496

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1249, CVE-2020-1353, CVE-2020-1370, CVE-2020-1399, CVE-2020-1404, CVE-2020-1413, CVE-2020-1414, CVE-2020-1422. **CVE ID : CVE-2020-1415**		
Improper Privilege Management	7/14/2020	9.3	An elevation of privilege vulnerability exists in Visual Studio and Visual Studio Code when they load software dependencies, aka 'Visual Studio and Visual Studio Code Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1416**	N/A	O-MIC-WIND-100820/1497
Improper Input Validation	7/14/2020	7.2	An elevation of privilege vulnerability exists when the Windows Diagnostics Execution Service fails to properly sanitize input, leading to an unsecure library-loading behavior, aka 'Windows Diagnostics Hub Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1393. **CVE ID : CVE-2020-1418**	N/A	O-MIC-WIND-100820/1498
Improper Restriction of Operations within the	7/14/2020	2.1	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a	N/A	O-MIC-WIND-100820/1499

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			memory address, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1367, CVE-2020-1389, CVE-2020-1426. **CVE ID : CVE-2020-1419**		
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists when Windows Error Reporting improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Error Reporting Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1420**	N/A	O-MIC-WIND-100820/1500
Access of Resource Using Incompatible Type ('Type Confusion')	7/14/2020	9.3	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1421**	N/A	O-MIC-WIND-100820/1501
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows	N/A	O-MIC-WIND-100820/1502

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1249, CVE-2020-1353, CVE-2020-1370, CVE-2020-1399, CVE-2020-1404, CVE-2020-1413, CVE-2020-1414, CVE-2020-1415. **CVE ID : CVE-2020-1422**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Subsystem for Linux handles files, aka 'Windows Subsystem for Linux Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1423**	N/A	O-MIC-WIND-100820/1503
Improper Privilege Management	7/14/2020	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'. **CVE ID : CVE-2020-1424**	N/A	O-MIC-WIND-100820/1504
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1367, CVE-2020-1389, CVE-2020-1419.	N/A	O-MIC-WIND-100820/1505

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1426		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1390, CVE-2020-1428, CVE-2020-1438. **CVE ID : CVE-2020-1427**	N/A	O-MIC-WIND-100820/1506
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1390, CVE-2020-1427, CVE-2020-1438. **CVE ID : CVE-2020-1428**	N/A	O-MIC-WIND-100820/1507
Improper Privilege Management	7/14/2020	7.2	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles a process crash, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1429**	N/A	O-MIC-WIND-100820/1508

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows UPnP Device Host Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1354. **CVE ID : CVE-2020-1430**	N/A	O-MIC-WIND-100820/1509
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows AppX Deployment Extensions improperly performs privilege management, resulting in access to system files.To exploit this vulnerability, an authenticated attacker would need to run a specially crafted application to elevate privileges.The security update addresses the vulnerability by correcting how AppX Deployment Extensions manages privileges., aka 'Windows AppX Deployment Extensions Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1431**	N/A	O-MIC-WIND-100820/1510
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists when	N/A	O-MIC-WIND-100820/1511

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Skype for Business is accessed via Internet Explorer, aka 'Skype for Business via Internet Explorer Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1432**		
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists when Microsoft Edge PDF Reader improperly handles objects in memory, aka 'Microsoft Edge PDF Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1433**	N/A	O-MIC-WIND-100820/1512
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Sync Host Service handles objects in memory, aka 'Windows Sync Host Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1434**	N/A	O-MIC-WIND-100820/1513
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	9.3	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1435**	N/A	O-MIC-WIND-100820/1514
Improper Input Validation	7/14/2020	6.8	A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted fonts.For	N/A	O-MIC-WIND-100820/1515

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			all systems except Windows 10, an attacker who successfully exploited the vulnerability could execute code remotely, aka 'Windows Font Library Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1436**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Location Awareness Service handles objects in memory, aka 'Windows Network Location Awareness Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1437**	N/A	O-MIC-WIND-100820/1516
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1390, CVE-2020-1427, CVE-2020-1428. **CVE ID : CVE-2020-1438**	N/A	O-MIC-WIND-100820/1517
Improper Privilege Management	7/14/2020	3.6	An elevation of privilege vulnerability exists when the MpSigStub.exe for Defender allows file deletion in arbitrary	N/A	O-MIC-WIND-100820/1518

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Defender Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1461**		
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists when Skype for Business is accessed via Microsoft Edge (EdgeHTML-based), aka 'Skype for Business via Microsoft Edge (EdgeHTML-based) Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1462**	N/A	O-MIC-WIND-100820/1519
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the SharedStream Library handles objects in memory, aka 'Windows SharedStream Library Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1463**	N/A	O-MIC-WIND-100820/1520
Information Exposure	7/14/2020	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'. **CVE ID : CVE-2020-1468**	N/A	O-MIC-WIND-100820/1521
windows_7					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1085**	N/A	O-MIC-WIND-100820/1522
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1427, CVE-2020-1428, CVE-2020-1438. **CVE ID : CVE-2020-1390**	N/A	O-MIC-WIND-100820/1523
N/A	7/14/2020	6.8	A remote code execution vulnerability exists in .NET Framework, Microsoft SharePoint, and Visual Studio when the software fails to check the source markup of XML file input, aka '.NET Framework, SharePoint Server, and Visual Studio Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1147**	N/A	O-MIC-WIND-100820/1524
Improper Input Validation	7/14/2020	4	This security update corrects a denial of service in the Local Security	N/A	O-MIC-WIND-100820/1525

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Authority Subsystem Service (LSASS) caused when an authenticated attacker sends a specially crafted authentication request, aka 'Local Security Authority Subsystem Service Denial of Service Vulnerability'. **CVE ID : CVE-2020-1267**		
Improper Privilege Management	7/14/2020	3.7	An elevation of privilege vulnerability exists when Group Policy Services Policy Processing improperly handle reparse points, aka 'Group Policy Services Policy Processing Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1333**	N/A	O-MIC-WIND-100820/1526
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Modules Installer improperly handles file operations, aka 'Windows Modules Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1346**	N/A	O-MIC-WIND-100820/1527
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists when the Windows Graphics component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1351**	N/A	O-MIC-WIND-100820/1528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows UPnP Device Host Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1430. **CVE ID : CVE-2020-1354**	N/A	O-MIC-WIND-100820/1529
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Cryptography Next Generation (CNG) Key Isolation service improperly handles memory, aka 'Windows CNG Key Isolation Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1384. **CVE ID : CVE-2020-1359**	N/A	O-MIC-WIND-100820/1530
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Profile Service improperly handles file operations, aka 'Windows Profile Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1360**	N/A	O-MIC-WIND-100820/1531
Improper	7/14/2020	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 Event Logging Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Event Logging Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1371. **CVE ID : CVE-2020-1365**		100820/1532
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Event Logging Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Event Logging Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1365. **CVE ID : CVE-2020-1371**	N/A	O-MIC-WIND-100820/1533
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'.	N/A	O-MIC-WIND-100820/1534

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This CVE ID is unique from CVE-2020-1390, CVE-2020-1427, CVE-2020-1428, CVE-2020-1438. **CVE ID : CVE-2020-1373**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	5.1	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1374**	N/A	O-MIC-WIND-100820/1535
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Cryptography Next Generation (CNG) Key Isolation service improperly handles memory, aka 'Windows CNG Key Isolation Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1359. **CVE ID : CVE-2020-1384**	N/A	O-MIC-WIND-100820/1536
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1367, CVE-2020-1419,	N/A	O-MIC-WIND-100820/1537

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-1426. **CVE ID : CVE-2020-1389**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to Advanced Local Procedure Call (ALPC).An attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the local system, aka 'Windows ALPC Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1396**	N/A	O-MIC-WIND-100820/1538
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists in Windows when the Windows Imaging Component fails to properly handle objects in memory, aka 'Windows Imaging Component Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1397**	N/A	O-MIC-WIND-100820/1539
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	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-2020-1401, CVE-2020-1407. **CVE ID : CVE-2020-1400**	N/A	O-MIC-WIND-100820/1540

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	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-2020-1400, CVE-2020-1407. **CVE ID : CVE-2020-1401**	N/A	O-MIC-WIND-100820/1541
Improper Privilege Management	7/14/2020	7.2	An elevation of privilege vulnerability exists when the Windows ActiveX Installer Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows ActiveX Installer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1402**	N/A	O-MIC-WIND-100820/1542
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	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'. **CVE ID : CVE-2020-1403**	N/A	O-MIC-WIND-100820/1543
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	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-100820/1544

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1400, CVE-2020-1401. **CVE ID : CVE-2020-1407**		
Origin Validation Error	7/14/2020	9.3	A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Microsoft Graphics Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1408**	N/A	O-MIC-WIND-100820/1545
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	9.3	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1409**	N/A	O-MIC-WIND-100820/1546
N/A	7/14/2020	9.3	A remote code execution vulnerability exists when Windows Address Book (WAB) improperly processes vcard files.To exploit the vulnerability, an attacker could send a malicious vcard that a victim opens using Windows Address Book (WAB), aka 'Windows Address Book Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1410**	N/A	O-MIC-WIND-100820/1547

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	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-2020-1412**	N/A	O-MIC-WIND-100820/1548
Improper Privilege Management	7/14/2020	9.3	An elevation of privilege vulnerability exists in Visual Studio and Visual Studio Code when they load software dependencies, aka 'Visual Studio and Visual Studio Code Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1416**	N/A	O-MIC-WIND-100820/1549
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	2.1	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1367, CVE-2020-1389, CVE-2020-1426. **CVE ID : CVE-2020-1419**	N/A	O-MIC-WIND-100820/1550
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of	N/A	O-MIC-WIND-100820/1551

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1390, CVE-2020-1428, CVE-2020-1438. **CVE ID : CVE-2020-1427**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1390, CVE-2020-1427, CVE-2020-1438. **CVE ID : CVE-2020-1428**	N/A	O-MIC-WIND-100820/1552
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows UPnP Device Host Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1354. **CVE ID : CVE-2020-1430**	N/A	O-MIC-WIND-100820/1553
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists when Skype for Business is accessed via Internet	N/A	O-MIC-WIND-100820/1554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Explorer, aka 'Skype for Business via Internet Explorer Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1432**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	9.3	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1435**	N/A	O-MIC-WIND-100820/1555
Improper Input Validation	7/14/2020	6.8	A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted fonts.For all systems except Windows 10, an attacker who successfully exploited the vulnerability could execute code remotely, aka 'Windows Font Library Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1436**	N/A	O-MIC-WIND-100820/1556
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Location Awareness Service handles objects in memory, aka 'Windows Network Location Awareness Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1437**	N/A	O-MIC-WIND-100820/1557

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1390, CVE-2020-1427, CVE-2020-1428. **CVE ID : CVE-2020-1438**	N/A	O-MIC-WIND-100820/1558
Improper Privilege Management	7/14/2020	3.6	An elevation of privilege vulnerability exists when the MpSigStub.exe for Defender allows file deletion in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Defender Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1461**	N/A	O-MIC-WIND-100820/1559
Information Exposure	7/14/2020	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'. **CVE ID : CVE-2020-1468**	N/A	O-MIC-WIND-100820/1560
windows_8.1					
Improper Privilege	7/14/2020	4.6	An elevation of privilege vulnerability exists in the	N/A	O-MIC-WIND-100820/1561

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1085**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1427, CVE-2020-1428, CVE-2020-1438. **CVE ID : CVE-2020-1390**	N/A	O-MIC-WIND-100820/1562
N/A	7/14/2020	6.8	A remote code execution vulnerability exists in .NET Framework, Microsoft SharePoint, and Visual Studio when the software fails to check the source markup of XML file input, aka '.NET Framework, SharePoint Server, and Visual Studio Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1147**	N/A	O-MIC-WIND-100820/1563
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows	N/A	O-MIC-WIND-100820/1564

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1353, CVE-2020-1370, CVE-2020-1399, CVE-2020-1404, CVE-2020-1413, CVE-2020-1414, CVE-2020-1415, CVE-2020-1422. **CVE ID : CVE-2020-1249**		
Improper Input Validation	7/14/2020	4	This security update corrects a denial of service in the Local Security Authority Subsystem Service (LSASS) caused when an authenticated attacker sends a specially crafted authentication request, aka 'Local Security Authority Subsystem Service Denial of Service Vulnerability'. **CVE ID : CVE-2020-1267**	N/A	O-MIC-WIND-100820/1565
Improper Privilege Management	7/14/2020	3.7	An elevation of privilege vulnerability exists when Group Policy Services Policy Processing improperly handle reparse points, aka 'Group Policy Services Policy Processing Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1333**	N/A	O-MIC-WIND-100820/1566
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Modules Installer improperly handles file operations, aka 'Windows Modules	N/A	O-MIC-WIND-100820/1567

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1346**		
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists when the Windows Graphics component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1351**	N/A	O-MIC-WIND-100820/1568
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows UPnP Device Host Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1430. **CVE ID : CVE-2020-1354**	N/A	O-MIC-WIND-100820/1569
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Cryptography Next Generation (CNG) Key Isolation service improperly handles memory, aka 'Windows CNG Key Isolation Service Elevation of Privilege Vulnerability'. This CVE ID	N/A	O-MIC-WIND-100820/1570

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is unique from CVE-2020-1384. **CVE ID : CVE-2020-1359**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Profile Service improperly handles file operations, aka 'Windows Profile Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1360**	N/A	O-MIC-WIND-100820/1571
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Event Logging Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Event Logging Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1371. **CVE ID : CVE-2020-1365**	N/A	O-MIC-WIND-100820/1572
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Credential Enrollment Manager service handles objects in memory, aka 'Windows Credential Enrollment Manager Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1368**	N/A	O-MIC-WIND-100820/1573

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Event Logging Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Event Logging Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1365. **CVE ID : CVE-2020-1371**	N/A	O-MIC-WIND-100820/1574
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1390, CVE-2020-1427, CVE-2020-1428, CVE-2020-1438. **CVE ID : CVE-2020-1373**	N/A	O-MIC-WIND-100820/1575
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	5.1	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'.	N/A	O-MIC-WIND-100820/1576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1374		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Cryptography Next Generation (CNG) Key Isolation service improperly handles memory, aka 'Windows CNG Key Isolation Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1359. **CVE ID : CVE-2020-1384**	N/A	O-MIC-WIND-100820/1577
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Credential Picker handles objects in memory, aka 'Windows Credential Picker Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1385**	N/A	O-MIC-WIND-100820/1578
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1367, CVE-2020-1419, CVE-2020-1426. **CVE ID : CVE-2020-1389**	N/A	O-MIC-WIND-100820/1579
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when Windows improperly	N/A	O-MIC-WIND-100820/1580

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			handles calls to Advanced Local Procedure Call (ALPC).An attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the local system, aka 'Windows ALPC Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1396**		
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists in Windows when the Windows Imaging Component fails to properly handle objects in memory, aka 'Windows Imaging Component Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1397**	N/A	O-MIC-WIND-100820/1581
Improper Privilege Management	7/14/2020	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-2020-1249, CVE-2020-1353, CVE-2020-1370, CVE-2020-1404, CVE-2020-1413, CVE-2020-1414, CVE-2020-1415, CVE-2020-1422. **CVE ID : CVE-2020-1399**	N/A	O-MIC-WIND-100820/1582
Improper Restriction of	7/14/2020	9.3	A remote code execution vulnerability exists when	N/A	O-MIC-WIND-100820/1583

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1401, CVE-2020-1407. **CVE ID : CVE-2020-1400**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	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-2020-1400, CVE-2020-1407. **CVE ID : CVE-2020-1401**	N/A	O-MIC-WIND-100820/1584
Improper Privilege Management	7/14/2020	7.2	An elevation of privilege vulnerability exists when the Windows ActiveX Installer Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows ActiveX Installer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1402**	N/A	O-MIC-WIND-100820/1585
Improper Restriction of Operations within the Bounds of a	7/14/2020	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-100820/1586

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1403**		
Improper Privilege Management	7/14/2020	7.2	An elevation of privilege vulnerability exists in the way that the Windows Network List Service handles objects in memory, aka 'Windows Network List Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1406**	N/A	O-MIC-WIND-100820/1587
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	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-2020-1400, CVE-2020-1401. **CVE ID : CVE-2020-1407**	N/A	O-MIC-WIND-100820/1588
Origin Validation Error	7/14/2020	9.3	A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Microsoft Graphics Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1408**	N/A	O-MIC-WIND-100820/1589
Improper Restriction of Operations within the Bounds of a	7/14/2020	9.3	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite	N/A	O-MIC-WIND-100820/1590

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1409**		
N/A	7/14/2020	9.3	A remote code execution vulnerability exists when Windows Address Book (WAB) improperly processes vcard files.To exploit the vulnerability, an attacker could send a malicious vcard that a victim opens using Windows Address Book (WAB), aka 'Windows Address Book Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1410**	N/A	O-MIC-WIND-100820/1591
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	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-2020-1412**	N/A	O-MIC-WIND-100820/1592
Improper Privilege Management	7/14/2020	9.3	An elevation of privilege vulnerability exists in Visual Studio and Visual Studio Code when they load software dependencies, aka 'Visual Studio and Visual Studio Code Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1416**	N/A	O-MIC-WIND-100820/1593
Improper Restriction of	7/14/2020	2.1	An information disclosure vulnerability exists when	N/A	O-MIC-WIND-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			the Windows kernel fails to properly initialize a memory address, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1367, CVE-2020-1389, CVE-2020-1426. **CVE ID : CVE-2020-1419**		100820/1594
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1390, CVE-2020-1428, CVE-2020-1438. **CVE ID : CVE-2020-1427**	N/A	O-MIC-WIND-100820/1595
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1390, CVE-2020-1427, CVE-2020-1438. **CVE ID : CVE-2020-1428**	N/A	O-MIC-WIND-100820/1596
Improper	7/14/2020	4.6	An elevation of privilege	N/A	O-MIC-WIND-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			vulnerability exists when the Windows UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows UPnP Device Host Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1354. **CVE ID : CVE-2020-1430**		100820/1597
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists when Skype for Business is accessed via Internet Explorer, aka 'Skype for Business via Internet Explorer Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1432**	N/A	O-MIC-WIND-100820/1598
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	9.3	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1435**	N/A	O-MIC-WIND-100820/1599
Improper Input Validation	7/14/2020	6.8	A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted fonts.For all systems except Windows 10, an attacker	N/A	O-MIC-WIND-100820/1600

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			who successfully exploited the vulnerability could execute code remotely, aka 'Windows Font Library Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1436**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Location Awareness Service handles objects in memory, aka 'Windows Network Location Awareness Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1437**	N/A	O-MIC-WIND-100820/1601
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1390, CVE-2020-1427, CVE-2020-1428. **CVE ID : CVE-2020-1438**	N/A	O-MIC-WIND-100820/1602
Improper Privilege Management	7/14/2020	3.6	An elevation of privilege vulnerability exists when the MpSigStub.exe for Defender allows file deletion in arbitrary locations.To exploit the vulnerability, an attacker	N/A	O-MIC-WIND-100820/1603

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			would first have to log on to the system, aka 'Microsoft Defender Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1461**		
Information Exposure	7/14/2020	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'. **CVE ID : CVE-2020-1468**	N/A	O-MIC-WIND-100820/1604
windows_rt_8.1					
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1085**	N/A	O-MIC-WIND-100820/1605
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1427, CVE-2020-1428, CVE-2020-1438.	N/A	O-MIC-WIND-100820/1606

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1390		
N/A	7/14/2020	6.8	A remote code execution vulnerability exists in .NET Framework, Microsoft SharePoint, and Visual Studio when the software fails to check the source markup of XML file input, aka '.NET Framework, SharePoint Server, and Visual Studio Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1147**	N/A	O-MIC-WIND-100820/1607
Improper Privilege Management	7/14/2020	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-2020-1353, CVE-2020-1370, CVE-2020-1399, CVE-2020-1404, CVE-2020-1413, CVE-2020-1414, CVE-2020-1415, CVE-2020-1422. **CVE ID : CVE-2020-1249**	N/A	O-MIC-WIND-100820/1608
Improper Input Validation	7/14/2020	4	This security update corrects a denial of service in the Local Security Authority Subsystem Service (LSASS) caused when an authenticated attacker sends a specially crafted authentication request, aka 'Local Security Authority Subsystem Service Denial of Service	N/A	O-MIC-WIND-100820/1609

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. **CVE ID : CVE-2020-1267**		
Improper Privilege Management	7/14/2020	3.7	An elevation of privilege vulnerability exists when Group Policy Services Policy Processing improperly handle reparse points, aka 'Group Policy Services Policy Processing Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1333**	N/A	O-MIC-WIND-100820/1610
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Modules Installer improperly handles file operations, aka 'Windows Modules Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1346**	N/A	O-MIC-WIND-100820/1611
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists when the Windows Graphics component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1351**	N/A	O-MIC-WIND-100820/1612
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim	N/A	O-MIC-WIND-100820/1613

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system, aka 'Windows UPnP Device Host Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1430. **CVE ID : CVE-2020-1354**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Cryptography Next Generation (CNG) Key Isolation service improperly handles memory, aka 'Windows CNG Key Isolation Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1384. **CVE ID : CVE-2020-1359**	N/A	O-MIC-WIND-100820/1614
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Profile Service improperly handles file operations, aka 'Windows Profile Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1360**	N/A	O-MIC-WIND-100820/1615
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Event Logging Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim	N/A	O-MIC-WIND-100820/1616

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system, aka 'Windows Event Logging Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1371. **CVE ID : CVE-2020-1365**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Credential Enrollment Manager service handles objects in memory, aka 'Windows Credential Enrollment Manager Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1368**	N/A	O-MIC-WIND-100820/1617
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Event Logging Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Event Logging Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1365. **CVE ID : CVE-2020-1371**	N/A	O-MIC-WIND-100820/1618
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows	N/A	O-MIC-WIND-100820/1619

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1390, CVE-2020-1427, CVE-2020-1428, CVE-2020-1438. **CVE ID : CVE-2020-1373**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	5.1	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1374**	N/A	O-MIC-WIND-100820/1620
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Cryptography Next Generation (CNG) Key Isolation service improperly handles memory, aka 'Windows CNG Key Isolation Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1359. **CVE ID : CVE-2020-1384**	N/A	O-MIC-WIND-100820/1621
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Credential Picker handles objects in memory, aka 'Windows Credential Picker Elevation of	N/A	O-MIC-WIND-100820/1622

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability'. **CVE ID : CVE-2020-1385**		
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1367, CVE-2020-1419, CVE-2020-1426. **CVE ID : CVE-2020-1389**	N/A	O-MIC-WIND-100820/1623
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to Advanced Local Procedure Call (ALPC).An attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the local system, aka 'Windows ALPC Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1396**	N/A	O-MIC-WIND-100820/1624
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists in Windows when the Windows Imaging Component fails to properly handle objects in memory, aka 'Windows Imaging Component Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1397**	N/A	O-MIC-WIND-100820/1625

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	7/14/2020	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-2020-1249, CVE-2020-1353, CVE-2020-1370, CVE-2020-1404, CVE-2020-1413, CVE-2020-1414, CVE-2020-1415, CVE-2020-1422. **CVE ID : CVE-2020-1399**	N/A	O-MIC-WIND-100820/1626
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	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-2020-1401, CVE-2020-1407. **CVE ID : CVE-2020-1400**	N/A	O-MIC-WIND-100820/1627
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	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-2020-1400, CVE-2020-1407. **CVE ID : CVE-2020-1401**	N/A	O-MIC-WIND-100820/1628
Improper Privilege	7/14/2020	7.2	An elevation of privilege vulnerability exists when	N/A	O-MIC-WIND-100820/1629

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			the Windows ActiveX Installer Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows ActiveX Installer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1402**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	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'. **CVE ID : CVE-2020-1403**	N/A	O-MIC-WIND-100820/1630
Improper Privilege Management	7/14/2020	7.2	An elevation of privilege vulnerability exists in the way that the Windows Network List Service handles objects in memory, aka 'Windows Network List Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1406**	N/A	O-MIC-WIND-100820/1631
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	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-	N/A	O-MIC-WIND-100820/1632

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1400, CVE-2020-1401. **CVE ID : CVE-2020-1407**		
Origin Validation Error	7/14/2020	9.3	A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Microsoft Graphics Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1408**	N/A	O-MIC-WIND-100820/1633
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	9.3	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1409**	N/A	O-MIC-WIND-100820/1634
N/A	7/14/2020	9.3	A remote code execution vulnerability exists when Windows Address Book (WAB) improperly processes vcard files.To exploit the vulnerability, an attacker could send a malicious vcard that a victim opens using Windows Address Book (WAB), aka 'Windows Address Book Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1410**	N/A	O-MIC-WIND-100820/1635
Improper Restriction of Operations within the	7/14/2020	9.3	A remote code execution vulnerability exists in the way that Microsoft Graphics Components	N/A	O-MIC-WIND-100820/1636

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			handle objects in memory, aka 'Microsoft Graphics Components Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1412**		
Improper Privilege Management	7/14/2020	9.3	An elevation of privilege vulnerability exists in Visual Studio and Visual Studio Code when they load software dependencies, aka 'Visual Studio and Visual Studio Code Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1416**	N/A	O-MIC-WIND-100820/1637
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	2.1	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1367, CVE-2020-1389, CVE-2020-1426. **CVE ID : CVE-2020-1419**	N/A	O-MIC-WIND-100820/1638
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1390, CVE-2020-	N/A	O-MIC-WIND-100820/1639

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1428, CVE-2020-1438. **CVE ID : CVE-2020-1427**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1390, CVE-2020-1427, CVE-2020-1438. **CVE ID : CVE-2020-1428**	N/A	O-MIC-WIND-100820/1640
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows UPnP Device Host Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1354. **CVE ID : CVE-2020-1430**	N/A	O-MIC-WIND-100820/1641
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists when Skype for Business is accessed via Internet Explorer, aka 'Skype for Business via Internet Explorer Information Disclosure Vulnerability'.	N/A	O-MIC-WIND-100820/1642

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1432		
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	9.3	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1435**	N/A	O-MIC-WIND-100820/1643
Improper Input Validation	7/14/2020	6.8	A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted fonts.For all systems except Windows 10, an attacker who successfully exploited the vulnerability could execute code remotely, aka 'Windows Font Library Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1436**	N/A	O-MIC-WIND-100820/1644
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Location Awareness Service handles objects in memory, aka 'Windows Network Location Awareness Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1437**	N/A	O-MIC-WIND-100820/1645
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections	N/A	O-MIC-WIND-100820/1646

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1390, CVE-2020-1427, CVE-2020-1428. **CVE ID : CVE-2020-1438**		
Improper Privilege Management	7/14/2020	3.6	An elevation of privilege vulnerability exists when the MpSigStub.exe for Defender allows file deletion in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Defender Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1461**	N/A	O-MIC-WIND-100820/1647
Information Exposure	7/14/2020	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'. **CVE ID : CVE-2020-1468**	N/A	O-MIC-WIND-100820/1648
windows_server_2008					
Improper Input Validation	7/14/2020	7.7	A remote code execution vulnerability exists when Hyper-V RemoteFX vGPU on a host server fails to properly validate input from an authenticated user	https://nvidia.custhelp.com/app/answers/detail/a_id/5044	O-MIC-WIND-100820/1649

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on a guest operating system, aka 'Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1032, CVE-2020-1036, CVE-2020-1040, CVE-2020-1041, CVE-2020-1043. **CVE ID : CVE-2020-1042**		
Improper Input Validation	7/14/2020	7.7	A remote code execution vulnerability exists when Hyper-V RemoteFX vGPU on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1032, CVE-2020-1036, CVE-2020-1040, CVE-2020-1041, CVE-2020-1042. **CVE ID : CVE-2020-1043**	https://nvidia.custhelp.com/app/answers/detail/a_id/5044	O-MIC-WIND-100820/1650
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1085**	N/A	O-MIC-WIND-100820/1651
Improper	7/14/2020	4.6	An elevation of privilege	N/A	O-MIC-WIND-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1427, CVE-2020-1428, CVE-2020-1438. **CVE ID : CVE-2020-1390**		100820/1652
Improper Input Validation	7/14/2020	7.7	A remote code execution vulnerability exists when Hyper-V RemoteFX vGPU on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1036, CVE-2020-1040, CVE-2020-1041, CVE-2020-1042, CVE-2020-1043. **CVE ID : CVE-2020-1032**	https://nvidia.custhelp.com/app/answers/detail/a_id/5044	O-MIC-WIND-100820/1653
Improper Input Validation	7/14/2020	7.7	A remote code execution vulnerability exists when Hyper-V RemoteFX vGPU on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Hyper-V RemoteFX vGPU Remote Code Execution	https://nvidia.custhelp.com/app/answers/detail/a_id/5044	O-MIC-WIND-100820/1654

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. This CVE ID is unique from CVE-2020-1032, CVE-2020-1040, CVE-2020-1041, CVE-2020-1042, CVE-2020-1043. **CVE ID : CVE-2020-1036**		
Improper Input Validation	7/14/2020	7.7	A remote code execution vulnerability exists when Hyper-V RemoteFX vGPU on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1032, CVE-2020-1036, CVE-2020-1041, CVE-2020-1042, CVE-2020-1043. **CVE ID : CVE-2020-1040**	https://nvidia.custhelp.com/app/answers/detail/a_id/5044	O-MIC-WIND-100820/1655
Improper Input Validation	7/14/2020	7.7	A remote code execution vulnerability exists when Hyper-V RemoteFX vGPU on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1032, CVE-2020-1036, CVE-2020-1040, CVE-2020-1042, CVE-2020-1043.	https://nvidia.custhelp.com/app/answers/detail/a_id/5044	O-MIC-WIND-100820/1656

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1041		
N/A	7/14/2020	6.8	A remote code execution vulnerability exists in .NET Framework, Microsoft SharePoint, and Visual Studio when the software fails to check the source markup of XML file input, aka '.NET Framework, SharePoint Server, and Visual Studio Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1147**	N/A	O-MIC-WIND-100820/1657
Improper Input Validation	7/14/2020	4	This security update corrects a denial of service in the Local Security Authority Subsystem Service (LSASS) caused when an authenticated attacker sends a specially crafted authentication request, aka 'Local Security Authority Subsystem Service Denial of Service Vulnerability'. **CVE ID : CVE-2020-1267**	N/A	O-MIC-WIND-100820/1658
Improper Privilege Management	7/14/2020	3.7	An elevation of privilege vulnerability exists when Group Policy Services Policy Processing improperly handle reparse points, aka 'Group Policy Services Policy Processing Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1333**	N/A	O-MIC-WIND-100820/1659
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Modules	N/A	O-MIC-WIND-100820/1660

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Installer improperly handles file operations, aka 'Windows Modules Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1346**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	10	A remote code execution vulnerability exists in Windows Domain Name System servers when they fail to properly handle requests, aka 'Windows DNS Server Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1350**	N/A	O-MIC-WIND-100820/1661
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists when the Windows Graphics component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1351**	N/A	O-MIC-WIND-100820/1662
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows UPnP Device Host Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1430.	N/A	O-MIC-WIND-100820/1663

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1354		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Cryptography Next Generation (CNG) Key Isolation service improperly handles memory, aka 'Windows CNG Key Isolation Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1384. **CVE ID : CVE-2020-1359**	N/A	O-MIC-WIND-100820/1664
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Profile Service improperly handles file operations, aka 'Windows Profile Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1360**	N/A	O-MIC-WIND-100820/1665
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Event Logging Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Event Logging Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1371.	N/A	O-MIC-WIND-100820/1666

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1365		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Event Logging Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Event Logging Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1365. **CVE ID : CVE-2020-1371**	N/A	O-MIC-WIND-100820/1667
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1390, CVE-2020-1427, CVE-2020-1428, CVE-2020-1438. **CVE ID : CVE-2020-1373**	N/A	O-MIC-WIND-100820/1668
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	5.1	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution	N/A	O-MIC-WIND-100820/1669

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. **CVE ID : CVE-2020-1374**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Cryptography Next Generation (CNG) Key Isolation service improperly handles memory, aka 'Windows CNG Key Isolation Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1359. **CVE ID : CVE-2020-1384**	N/A	O-MIC-WIND-100820/1670
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1367, CVE-2020-1419, CVE-2020-1426. **CVE ID : CVE-2020-1389**	N/A	O-MIC-WIND-100820/1671
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to Advanced Local Procedure Call (ALPC).An attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the local system, aka	N/A	O-MIC-WIND-100820/1672

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			'Windows ALPC Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1396**		
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists in Windows when the Windows Imaging Component fails to properly handle objects in memory, aka 'Windows Imaging Component Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1397**	N/A	O-MIC-WIND-100820/1673
Improper Privilege Management	7/14/2020	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-2020-1249, CVE-2020-1353, CVE-2020-1370, CVE-2020-1404, CVE-2020-1413, CVE-2020-1414, CVE-2020-1415, CVE-2020-1422. **CVE ID : CVE-2020-1399**	N/A	O-MIC-WIND-100820/1674
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	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-2020-1401, CVE-2020-1407.	N/A	O-MIC-WIND-100820/1675

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1400		
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	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-2020-1400, CVE-2020-1407. **CVE ID : CVE-2020-1401**	N/A	O-MIC-WIND-100820/1676
Improper Privilege Management	7/14/2020	7.2	An elevation of privilege vulnerability exists when the Windows ActiveX Installer Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows ActiveX Installer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1402**	N/A	O-MIC-WIND-100820/1677
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	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'. **CVE ID : CVE-2020-1403**	N/A	O-MIC-WIND-100820/1678
Improper Restriction of Operations within the Bounds of a	7/14/2020	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-100820/1679

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-2020-1400, CVE-2020-1401. **CVE ID : CVE-2020-1407**		
Origin Validation Error	7/14/2020	9.3	A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Microsoft Graphics Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1408**	N/A	O-MIC-WIND-100820/1680
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	9.3	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1409**	N/A	O-MIC-WIND-100820/1681
N/A	7/14/2020	9.3	A remote code execution vulnerability exists when Windows Address Book (WAB) improperly processes vcard files.To exploit the vulnerability, an attacker could send a malicious vcard that a victim opens using Windows Address Book (WAB), aka 'Windows Address Book Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1410**	N/A	O-MIC-WIND-100820/1682

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	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-2020-1412**	N/A	O-MIC-WIND-100820/1683
Improper Privilege Management	7/14/2020	9.3	An elevation of privilege vulnerability exists in Visual Studio and Visual Studio Code when they load software dependencies, aka 'Visual Studio and Visual Studio Code Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1416**	N/A	O-MIC-WIND-100820/1684
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	2.1	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1367, CVE-2020-1389, CVE-2020-1426. **CVE ID : CVE-2020-1419**	N/A	O-MIC-WIND-100820/1685
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of	N/A	O-MIC-WIND-100820/1686

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1390, CVE-2020-1428, CVE-2020-1438. **CVE ID : CVE-2020-1427**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1390, CVE-2020-1427, CVE-2020-1438. **CVE ID : CVE-2020-1428**	N/A	O-MIC-WIND-100820/1687
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows UPnP Device Host Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1354. **CVE ID : CVE-2020-1430**	N/A	O-MIC-WIND-100820/1688
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists when Skype for Business is accessed via Internet	N/A	O-MIC-WIND-100820/1689

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Explorer, aka 'Skype for Business via Internet Explorer Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1432**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	9.3	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1435**	N/A	O-MIC-WIND-100820/1690
Improper Input Validation	7/14/2020	6.8	A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted fonts.For all systems except Windows 10, an attacker who successfully exploited the vulnerability could execute code remotely, aka 'Windows Font Library Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1436**	N/A	O-MIC-WIND-100820/1691
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Location Awareness Service handles objects in memory, aka 'Windows Network Location Awareness Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1437**	N/A	O-MIC-WIND-100820/1692

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1390, CVE-2020-1427, CVE-2020-1428. **CVE ID : CVE-2020-1438**	N/A	O-MIC-WIND-100820/1693
Improper Privilege Management	7/14/2020	3.6	An elevation of privilege vulnerability exists when the MpSigStub.exe for Defender allows file deletion in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Defender Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1461**	N/A	O-MIC-WIND-100820/1694
Information Exposure	7/14/2020	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'. **CVE ID : CVE-2020-1468**	N/A	O-MIC-WIND-100820/1695
windows_server_2012					
Improper Input Validation	7/14/2020	7.7	A remote code execution vulnerability exists when	https://nvidia.custhelp	O-MIC-WIND-100820/1696

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Hyper-V RemoteFX vGPU on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1032, CVE-2020-1036, CVE-2020-1040, CVE-2020-1041, CVE-2020-1043. **CVE ID : CVE-2020-1042**	.com/app/answers/detail/a_id/5044	
Improper Input Validation	7/14/2020	7.7	A remote code execution vulnerability exists when Hyper-V RemoteFX vGPU on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1032, CVE-2020-1036, CVE-2020-1040, CVE-2020-1041, CVE-2020-1042. **CVE ID : CVE-2020-1043**	https://nvidia.custhelp.com/app/answers/detail/a_id/5044	O-MIC-WIND-100820/1697
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege	N/A	O-MIC-WIND-100820/1698

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. **CVE ID : CVE-2020-1085**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1427, CVE-2020-1428, CVE-2020-1438. **CVE ID : CVE-2020-1390**	N/A	O-MIC-WIND-100820/1699
Improper Input Validation	7/14/2020	7.7	A remote code execution vulnerability exists when Hyper-V RemoteFX vGPU on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1036, CVE-2020-1040, CVE-2020-1041, CVE-2020-1042, CVE-2020-1043. **CVE ID : CVE-2020-1032**	https://nvidia.custhelp.com/app/answers/detail/a_id/5044	O-MIC-WIND-100820/1700
Improper Input Validation	7/14/2020	7.7	A remote code execution vulnerability exists when Hyper-V RemoteFX vGPU on a host server fails to properly validate input from an authenticated user	https://nvidia.custhelp.com/app/answers/detail/a_id/5044	O-MIC-WIND-100820/1701

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on a guest operating system, aka 'Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1032, CVE-2020-1040, CVE-2020-1041, CVE-2020-1042, CVE-2020-1043. **CVE ID : CVE-2020-1036**		
Improper Input Validation	7/14/2020	7.7	A remote code execution vulnerability exists when Hyper-V RemoteFX vGPU on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1032, CVE-2020-1036, CVE-2020-1041, CVE-2020-1042, CVE-2020-1043. **CVE ID : CVE-2020-1040**	https://nvidia.custhelp.com/app/answers/detail/a_id/5044	O-MIC-WIND-100820/1702
Improper Input Validation	7/14/2020	7.7	A remote code execution vulnerability exists when Hyper-V RemoteFX vGPU on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-	https://nvidia.custhelp.com/app/answers/detail/a_id/5044	O-MIC-WIND-100820/1703

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1032, CVE-2020-1036, CVE-2020-1040, CVE-2020-1042, CVE-2020-1043. **CVE ID : CVE-2020-1041**		
N/A	7/14/2020	6.8	A remote code execution vulnerability exists in .NET Framework, Microsoft SharePoint, and Visual Studio when the software fails to check the source markup of XML file input, aka '.NET Framework, SharePoint Server, and Visual Studio Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1147**	N/A	O-MIC-WIND-100820/1704
Improper Privilege Management	7/14/2020	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-2020-1353, CVE-2020-1370, CVE-2020-1399, CVE-2020-1404, CVE-2020-1413, CVE-2020-1414, CVE-2020-1415, CVE-2020-1422. **CVE ID : CVE-2020-1249**	N/A	O-MIC-WIND-100820/1705
Improper Input Validation	7/14/2020	4	This security update corrects a denial of service in the Local Security Authority Subsystem Service (LSASS) caused when an authenticated attacker sends a specially	N/A	O-MIC-WIND-100820/1706

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted authentication request, aka 'Local Security Authority Subsystem Service Denial of Service Vulnerability'. **CVE ID : CVE-2020-1267**		
Improper Privilege Management	7/14/2020	3.7	An elevation of privilege vulnerability exists when Group Policy Services Policy Processing improperly handle reparse points, aka 'Group Policy Services Policy Processing Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1333**	N/A	O-MIC-WIND-100820/1707
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Modules Installer improperly handles file operations, aka 'Windows Modules Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1346**	N/A	O-MIC-WIND-100820/1708
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	10	A remote code execution vulnerability exists in Windows Domain Name System servers when they fail to properly handle requests, aka 'Windows DNS Server Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1350**	N/A	O-MIC-WIND-100820/1709
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists when the Windows Graphics component improperly handles objects in	N/A	O-MIC-WIND-100820/1710

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1351**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows UPnP Device Host Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1430. **CVE ID : CVE-2020-1354**	N/A	O-MIC-WIND-100820/1711
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows iSCSI Target Service improperly handles file operations, aka 'Windows iSCSI Target Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1356**	N/A	O-MIC-WIND-100820/1712
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Cryptography Next Generation (CNG) Key Isolation service improperly handles memory, aka 'Windows CNG Key Isolation Service Elevation of Privilege	N/A	O-MIC-WIND-100820/1713

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. This CVE ID is unique from CVE-2020-1384. **CVE ID : CVE-2020-1359**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Profile Service improperly handles file operations, aka 'Windows Profile Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1360**	N/A	O-MIC-WIND-100820/1714
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Event Logging Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Event Logging Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1371. **CVE ID : CVE-2020-1365**	N/A	O-MIC-WIND-100820/1715
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Credential Enrollment Manager service handles objects in memory, aka 'Windows Credential Enrollment Manager Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1368**	N/A	O-MIC-WIND-100820/1716

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Event Logging Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Event Logging Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1365. **CVE ID : CVE-2020-1371**	N/A	O-MIC-WIND-100820/1717
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1390, CVE-2020-1427, CVE-2020-1428, CVE-2020-1438. **CVE ID : CVE-2020-1373**	N/A	O-MIC-WIND-100820/1718
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	5.1	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'.	N/A	O-MIC-WIND-100820/1719

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1374		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Cryptography Next Generation (CNG) Key Isolation service improperly handles memory, aka 'Windows CNG Key Isolation Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1359. **CVE ID : CVE-2020-1384**	N/A	O-MIC-WIND-100820/1720
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Credential Picker handles objects in memory, aka 'Windows Credential Picker Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1385**	N/A	O-MIC-WIND-100820/1721
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1367, CVE-2020-1419, CVE-2020-1426. **CVE ID : CVE-2020-1389**	N/A	O-MIC-WIND-100820/1722
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when Windows improperly	N/A	O-MIC-WIND-100820/1723

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			handles calls to Advanced Local Procedure Call (ALPC).An attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the local system, aka 'Windows ALPC Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1396**		
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists in Windows when the Windows Imaging Component fails to properly handle objects in memory, aka 'Windows Imaging Component Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1397**	N/A	O-MIC-WIND-100820/1724
Improper Privilege Management	7/14/2020	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-2020-1249, CVE-2020-1353, CVE-2020-1370, CVE-2020-1404, CVE-2020-1413, CVE-2020-1414, CVE-2020-1415, CVE-2020-1422. **CVE ID : CVE-2020-1399**	N/A	O-MIC-WIND-100820/1725
Improper Restriction of	7/14/2020	9.3	A remote code execution vulnerability exists when	N/A	O-MIC-WIND-100820/1726

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1401, CVE-2020-1407. **CVE ID : CVE-2020-1400**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	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-2020-1400, CVE-2020-1407. **CVE ID : CVE-2020-1401**	N/A	O-MIC-WIND-100820/1727
Improper Privilege Management	7/14/2020	7.2	An elevation of privilege vulnerability exists when the Windows ActiveX Installer Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows ActiveX Installer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1402**	N/A	O-MIC-WIND-100820/1728
Improper Restriction of Operations within the Bounds of a	7/14/2020	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-100820/1729

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1403**		
Improper Privilege Management	7/14/2020	7.2	An elevation of privilege vulnerability exists in the way that the Windows Network List Service handles objects in memory, aka 'Windows Network List Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1406**	N/A	O-MIC-WIND-100820/1730
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	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-2020-1400, CVE-2020-1401. **CVE ID : CVE-2020-1407**	N/A	O-MIC-WIND-100820/1731
Origin Validation Error	7/14/2020	9.3	A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Microsoft Graphics Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1408**	N/A	O-MIC-WIND-100820/1732
Improper Restriction of Operations within the Bounds of a	7/14/2020	9.3	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite	N/A	O-MIC-WIND-100820/1733

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1409**		
N/A	7/14/2020	9.3	A remote code execution vulnerability exists when Windows Address Book (WAB) improperly processes vcard files.To exploit the vulnerability, an attacker could send a malicious vcard that a victim opens using Windows Address Book (WAB), aka 'Windows Address Book Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1410**	N/A	O-MIC-WIND-100820/1734
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	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-2020-1412**	N/A	O-MIC-WIND-100820/1735
Improper Privilege Management	7/14/2020	9.3	An elevation of privilege vulnerability exists in Visual Studio and Visual Studio Code when they load software dependencies, aka 'Visual Studio and Visual Studio Code Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1416**	N/A	O-MIC-WIND-100820/1736
Improper Restriction of	7/14/2020	2.1	An information disclosure vulnerability exists when	N/A	O-MIC-WIND-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			the Windows kernel fails to properly initialize a memory address, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1367, CVE-2020-1389, CVE-2020-1426. **CVE ID : CVE-2020-1419**		100820/1737
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1390, CVE-2020-1428, CVE-2020-1438. **CVE ID : CVE-2020-1427**	N/A	O-MIC-WIND-100820/1738
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1390, CVE-2020-1427, CVE-2020-1438. **CVE ID : CVE-2020-1428**	N/A	O-MIC-WIND-100820/1739
Improper	7/14/2020	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 UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows UPnP Device Host Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1354. **CVE ID : CVE-2020-1430**		100820/1740
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists when Skype for Business is accessed via Internet Explorer, aka 'Skype for Business via Internet Explorer Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1432**	N/A	O-MIC-WIND-100820/1741
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	9.3	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1435**	N/A	O-MIC-WIND-100820/1742
Improper Input Validation	7/14/2020	6.8	A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted fonts.For all systems except Windows 10, an attacker	N/A	O-MIC-WIND-100820/1743

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			who successfully exploited the vulnerability could execute code remotely, aka 'Windows Font Library Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1436**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Location Awareness Service handles objects in memory, aka 'Windows Network Location Awareness Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1437**	N/A	O-MIC-WIND-100820/1744
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1390, CVE-2020-1427, CVE-2020-1428. **CVE ID : CVE-2020-1438**	N/A	O-MIC-WIND-100820/1745
Improper Privilege Management	7/14/2020	3.6	An elevation of privilege vulnerability exists when the MpSigStub.exe for Defender allows file deletion in arbitrary locations.To exploit the vulnerability, an attacker	N/A	O-MIC-WIND-100820/1746

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			would first have to log on to the system, aka 'Microsoft Defender Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1461**		
Information Exposure	7/14/2020	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'. **CVE ID : CVE-2020-1468**	N/A	O-MIC-WIND-100820/1747
windows_server_2016					
Improper Input Validation	7/14/2020	7.7	A remote code execution vulnerability exists when Hyper-V RemoteFX vGPU on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1032, CVE-2020-1036, CVE-2020-1040, CVE-2020-1041, CVE-2020-1043. **CVE ID : CVE-2020-1042**	https://nvidia.custhelp.com/app/answers/detail/a_id/5044	O-MIC-WIND-100820/1748
Improper Input Validation	7/14/2020	7.7	A remote code execution vulnerability exists when Hyper-V RemoteFX vGPU on a host server fails to properly validate input from an authenticated user	https://nvidia.custhelp.com/app/answers/detail/a_id/5044	O-MIC-WIND-100820/1749

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on a guest operating system, aka 'Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1032, CVE-2020-1036, CVE-2020-1040, CVE-2020-1041, CVE-2020-1042. **CVE ID : CVE-2020-1043**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1085**	N/A	O-MIC-WIND-100820/1750
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1427, CVE-2020-1428, CVE-2020-1438. **CVE ID : CVE-2020-1390**	N/A	O-MIC-WIND-100820/1751
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists when the Windows Agent Activation Runtime	N/A	O-MIC-WIND-100820/1752

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(AarSvc) fails to properly handle objects in memory, aka 'Windows Agent Activation Runtime Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1391**		
Improper Input Validation	7/14/2020	7.7	A remote code execution vulnerability exists when Hyper-V RemoteFX vGPU on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1036, CVE-2020-1040, CVE-2020-1041, CVE-2020-1042, CVE-2020-1043. **CVE ID : CVE-2020-1032**	https://nvidia.custhelp.com/app/answers/detail/a_id/5044	O-MIC-WIND-100820/1753
Improper Input Validation	7/14/2020	7.7	A remote code execution vulnerability exists when Hyper-V RemoteFX vGPU on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1032, CVE-2020-1040, CVE-2020-1041, CVE-2020-1042, CVE-2020-1043.	https://nvidia.custhelp.com/app/answers/detail/a_id/5044	O-MIC-WIND-100820/1754

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1036		
Improper Input Validation	7/14/2020	7.7	A remote code execution vulnerability exists when Hyper-V RemoteFX vGPU on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1032, CVE-2020-1036, CVE-2020-1041, CVE-2020-1042, CVE-2020-1043. **CVE ID : CVE-2020-1040**	https://nvidia.custhelp.com/app/answers/detail/a_id/5044	O-MIC-WIND-100820/1755
Improper Input Validation	7/14/2020	7.7	A remote code execution vulnerability exists when Hyper-V RemoteFX vGPU on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1032, CVE-2020-1036, CVE-2020-1040, CVE-2020-1042, CVE-2020-1043. **CVE ID : CVE-2020-1041**	https://nvidia.custhelp.com/app/answers/detail/a_id/5044	O-MIC-WIND-100820/1756
N/A	7/14/2020	6.8	A remote code execution vulnerability exists in .NET Framework, Microsoft SharePoint, and Visual Studio when the software	N/A	O-MIC-WIND-100820/1757

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			fails to check the source markup of XML file input, aka '.NET Framework, SharePoint Server, and Visual Studio Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1147**		
Improper Privilege Management	7/14/2020	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-2020-1353, CVE-2020-1370, CVE-2020-1399, CVE-2020-1404, CVE-2020-1413, CVE-2020-1414, CVE-2020-1415, CVE-2020-1422. **CVE ID : CVE-2020-1249**	N/A	O-MIC-WIND-100820/1758
Improper Input Validation	7/14/2020	4	This security update corrects a denial of service in the Local Security Authority Subsystem Service (LSASS) caused when an authenticated attacker sends a specially crafted authentication request, aka 'Local Security Authority Subsystem Service Denial of Service Vulnerability'. **CVE ID : CVE-2020-1267**	N/A	O-MIC-WIND-100820/1759
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists when Windows Mobile Device Management (MDM)	N/A	O-MIC-WIND-100820/1760

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Diagnostics improperly handles junctions, aka 'Windows Mobile Device Management Diagnostics Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1330**		
Improper Privilege Management	7/14/2020	3.7	An elevation of privilege vulnerability exists when Group Policy Services Policy Processing improperly handle reparse points, aka 'Group Policy Services Policy Processing Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1333**	N/A	O-MIC-WIND-100820/1761
Improper Privilege Management	7/14/2020	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-2020-1411. **CVE ID : CVE-2020-1336**	N/A	O-MIC-WIND-100820/1762
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows WalletService handles objects in memory, aka 'Windows WalletService Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1362, CVE-2020-1369. **CVE ID : CVE-2020-1344**	N/A	O-MIC-WIND-100820/1763

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Modules Installer improperly handles file operations, aka 'Windows Modules Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1346**	N/A	O-MIC-WIND-100820/1764
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Storage Services improperly handle file operations, aka 'Windows Storage Services Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1347**	N/A	O-MIC-WIND-100820/1765
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	10	A remote code execution vulnerability exists in Windows Domain Name System servers when they fail to properly handle requests, aka 'Windows DNS Server Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1350**	N/A	O-MIC-WIND-100820/1766
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists when the Windows Graphics component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1351**	N/A	O-MIC-WIND-100820/1767
Improper Privilege	7/14/2020	4.6	An elevation of privilege vulnerability exists when	N/A	O-MIC-WIND-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			the Windows USO Core Worker improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows USO Core Worker Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1352**		100820/1768
Improper Privilege Management	7/14/2020	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-2020-1249, CVE-2020-1370, CVE-2020-1399, CVE-2020-1404, CVE-2020-1413, CVE-2020-1414, CVE-2020-1415, CVE-2020-1422. **CVE ID : CVE-2020-1353**	N/A	O-MIC-WIND-100820/1769
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows UPnP Device Host Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1430.	N/A	O-MIC-WIND-100820/1770

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1354		
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	4.6	A remote code execution vulnerability exists when the Windows Font Driver Host improperly handles memory.An attacker who successfully exploited the vulnerability would gain execution on a victim system.The security update addresses the vulnerability by correcting how the Windows Font Driver Host handles memory., aka 'Windows Font Driver Host Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1355**	N/A	O-MIC-WIND-100820/1771
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows iSCSI Target Service improperly handles file operations, aka 'Windows iSCSI Target Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1356**	N/A	O-MIC-WIND-100820/1772
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows System Events Broker improperly handles file operations, aka 'Windows System Events Broker Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1357**	N/A	O-MIC-WIND-100820/1773
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists when	N/A	O-MIC-WIND-100820/1774

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the Windows Resource Policy component improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Resource Policy Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1358**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Cryptography Next Generation (CNG) Key Isolation service improperly handles memory, aka 'Windows CNG Key Isolation Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1384. **CVE ID : CVE-2020-1359**	N/A	O-MIC-WIND-100820/1775
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Profile Service improperly handles file operations, aka 'Windows Profile Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1360**	N/A	O-MIC-WIND-100820/1776
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists in the way that the WalletService handles memory.To exploit	N/A	O-MIC-WIND-100820/1777

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the vulnerability, an attacker would first need code execution on a victim system, aka 'Windows WalletService Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1361**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows WalletService handles objects in memory, aka 'Windows WalletService Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1344, CVE-2020-1369. **CVE ID : CVE-2020-1362**	N/A	O-MIC-WIND-100820/1778
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Picker Platform improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Picker Platform Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1363**	N/A	O-MIC-WIND-100820/1779
Improper Input Validation	7/14/2020	3.6	A denial of service vulnerability exists in the way that the WalletService handles files, aka 'Windows WalletService Denial of Service Vulnerability'. **CVE ID : CVE-2020-1364**	N/A	O-MIC-WIND-100820/1780

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Event Logging Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Event Logging Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1371. **CVE ID : CVE-2020-1365**	N/A	O-MIC-WIND-100820/1781
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Print Workflow Service improperly handles objects in memory, aka 'Windows Print Workflow Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1366**	N/A	O-MIC-WIND-100820/1782
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1389, CVE-2020-1419, CVE-2020-1426. **CVE ID : CVE-2020-1367**	N/A	O-MIC-WIND-100820/1783
Improper	7/14/2020	4.6	An elevation of privilege	N/A	O-MIC-WIND-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			vulnerability exists in the way that the Credential Enrollment Manager service handles objects in memory, aka 'Windows Credential Enrollment Manager Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1368**		100820/1784
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows WalletService handles objects in memory, aka 'Windows WalletService Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1344, CVE-2020-1362. **CVE ID : CVE-2020-1369**	N/A	O-MIC-WIND-100820/1785
Improper Privilege Management	7/14/2020	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-2020-1249, CVE-2020-1353, CVE-2020-1399, CVE-2020-1404, CVE-2020-1413, CVE-2020-1414, CVE-2020-1415, CVE-2020-1422. **CVE ID : CVE-2020-1370**	N/A	O-MIC-WIND-100820/1786
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Event Logging Service	N/A	O-MIC-WIND-100820/1787

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Event Logging Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1365. **CVE ID : CVE-2020-1371**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when Windows Mobile Device Management (MDM) Diagnostics improperly handles objects in memory, aka 'Windows Mobile Device Management Diagnostics Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1405. **CVE ID : CVE-2020-1372**	N/A	O-MIC-WIND-100820/1788
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1390, CVE-2020-1427, CVE-2020-1428, CVE-2020-1438.	N/A	O-MIC-WIND-100820/1789

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1373		
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	5.1	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1374**	N/A	O-MIC-WIND-100820/1790
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when Windows improperly handles COM object creation, aka 'Windows COM Server Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1375**	N/A	O-MIC-WIND-100820/1791
Use After Free	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1382. **CVE ID : CVE-2020-1381**	N/A	O-MIC-WIND-100820/1792
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege	N/A	O-MIC-WIND-100820/1793

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. This CVE ID is unique from CVE-2020-1381. **CVE ID : CVE-2020-1382**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Cryptography Next Generation (CNG) Key Isolation service improperly handles memory, aka 'Windows CNG Key Isolation Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1359. **CVE ID : CVE-2020-1384**	N/A	O-MIC-WIND-100820/1794
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Credential Picker handles objects in memory, aka 'Windows Credential Picker Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1385**	N/A	O-MIC-WIND-100820/1795
Information Exposure	7/14/2020	2.1	An information vulnerability exists when Windows Connected User Experiences and Telemetry Service improperly discloses file information, aka 'Connected User Experiences and Telemetry Service Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1386**	N/A	O-MIC-WIND-100820/1796

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	7/14/2020	4.6	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-2020-1387**	N/A	O-MIC-WIND-100820/1797
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the psmsrv.dll handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1392, CVE-2020-1394, CVE-2020-1395. **CVE ID : CVE-2020-1388**	N/A	O-MIC-WIND-100820/1798
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1367, CVE-2020-1419, CVE-2020-1426. **CVE ID : CVE-2020-1389**	N/A	O-MIC-WIND-100820/1799
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Delivery Optimization service improperly handles objects in memory, aka 'Windows	N/A	O-MIC-WIND-100820/1800

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1388, CVE-2020-1394, CVE-2020-1395. **CVE ID : CVE-2020-1392**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Diagnostics Hub Standard Collector Service fails to properly sanitize input, leading to an unsecure library-loading behavior, aka 'Windows Diagnostics Hub Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1418. **CVE ID : CVE-2020-1393**	N/A	O-MIC-WIND-100820/1801
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Geolocation Framework handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1388, CVE-2020-1392, CVE-2020-1395. **CVE ID : CVE-2020-1394**	N/A	O-MIC-WIND-100820/1802
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Speech Brokered API handles objects in memory, aka 'Windows Elevation of Privilege	N/A	O-MIC-WIND-100820/1803

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. This CVE ID is unique from CVE-2020-1388, CVE-2020-1392, CVE-2020-1394. **CVE ID : CVE-2020-1395**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to Advanced Local Procedure Call (ALPC).An attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the local system, aka 'Windows ALPC Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1396**	N/A	O-MIC-WIND-100820/1804
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists in Windows when the Windows Imaging Component fails to properly handle objects in memory, aka 'Windows Imaging Component Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1397**	N/A	O-MIC-WIND-100820/1805
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when Windows Lockscreen fails to properly handle Ease of Access dialog.An attacker who successfully exploited the vulnerability could execute commands with elevated permissions.The	N/A	O-MIC-WIND-100820/1806

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			security update addresses the vulnerability by ensuring that the Ease of Access dialog is handled properly., aka 'Windows Lockscreen Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1398**		
Improper Privilege Management	7/14/2020	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-2020-1249, CVE-2020-1353, CVE-2020-1370, CVE-2020-1404, CVE-2020-1413, CVE-2020-1414, CVE-2020-1415, CVE-2020-1422. **CVE ID : CVE-2020-1399**	N/A	O-MIC-WIND-100820/1807
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	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-2020-1401, CVE-2020-1407. **CVE ID : CVE-2020-1400**	N/A	O-MIC-WIND-100820/1808
Improper Restriction of Operations within the Bounds of a	7/14/2020	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-100820/1809

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-2020-1400, CVE-2020-1407. **CVE ID : CVE-2020-1401**		
Improper Privilege Management	7/14/2020	7.2	An elevation of privilege vulnerability exists when the Windows ActiveX Installer Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows ActiveX Installer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1402**	N/A	O-MIC-WIND-100820/1810
Improper Privilege Management	7/14/2020	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-2020-1249, CVE-2020-1353, CVE-2020-1370, CVE-2020-1399, CVE-2020-1413, CVE-2020-1414, CVE-2020-1415, CVE-2020-1422. **CVE ID : CVE-2020-1404**	N/A	O-MIC-WIND-100820/1811
Improper Privilege Management	7/14/2020	3.6	An elevation of privilege vulnerability exists when Windows Mobile Device Management (MDM)	N/A	O-MIC-WIND-100820/1812

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Diagnostics improperly handles junctions, aka 'Windows Mobile Device Management Diagnostics Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1372. **CVE ID : CVE-2020-1405**		
Improper Privilege Management	7/14/2020	7.2	An elevation of privilege vulnerability exists in the way that the Windows Network List Service handles objects in memory, aka 'Windows Network List Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1406**	N/A	O-MIC-WIND-100820/1813
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	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-2020-1400, CVE-2020-1401. **CVE ID : CVE-2020-1407**	N/A	O-MIC-WIND-100820/1814
Origin Validation Error	7/14/2020	9.3	A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Microsoft Graphics Remote Code Execution Vulnerability'.	N/A	O-MIC-WIND-100820/1815

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1408		
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	9.3	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1409**	N/A	O-MIC-WIND-100820/1816
N/A	7/14/2020	9.3	A remote code execution vulnerability exists when Windows Address Book (WAB) improperly processes vcard files.To exploit the vulnerability, an attacker could send a malicious vcard that a victim opens using Windows Address Book (WAB), aka 'Windows Address Book Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1410**	N/A	O-MIC-WIND-100820/1817
Improper Privilege Management	7/14/2020	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-2020-1336. **CVE ID : CVE-2020-1411**	N/A	O-MIC-WIND-100820/1818
Improper Restriction of Operations within the Bounds of a	7/14/2020	9.3	A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory,	N/A	O-MIC-WIND-100820/1819

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer		🟥	aka 'Microsoft Graphics Components Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1412**		
Improper Privilege Management	7/14/2020	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-2020-1249, CVE-2020-1353, CVE-2020-1370, CVE-2020-1399, CVE-2020-1404, CVE-2020-1414, CVE-2020-1415, CVE-2020-1422. **CVE ID : CVE-2020-1413**	N/A	O-MIC-WIND-100820/1820
Improper Privilege Management	7/14/2020	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-2020-1249, CVE-2020-1353, CVE-2020-1370, CVE-2020-1399, CVE-2020-1404, CVE-2020-1413, CVE-2020-1415, CVE-2020-1422. **CVE ID : CVE-2020-1414**	N/A	O-MIC-WIND-100820/1821
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows	N/A	O-MIC-WIND-100820/1822

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1249, CVE-2020-1353, CVE-2020-1370, CVE-2020-1399, CVE-2020-1404, CVE-2020-1413, CVE-2020-1414, CVE-2020-1422. **CVE ID : CVE-2020-1415**		
Improper Privilege Management	7/14/2020	9.3	An elevation of privilege vulnerability exists in Visual Studio and Visual Studio Code when they load software dependencies, aka 'Visual Studio and Visual Studio Code Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1416**	N/A	O-MIC-WIND-100820/1823
Improper Input Validation	7/14/2020	7.2	An elevation of privilege vulnerability exists when the Windows Diagnostics Execution Service fails to properly sanitize input, leading to an unsecure library-loading behavior, aka 'Windows Diagnostics Hub Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1393. **CVE ID : CVE-2020-1418**	N/A	O-MIC-WIND-100820/1824
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	2.1	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address, aka 'Windows Kernel	N/A	O-MIC-WIND-100820/1825

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1367, CVE-2020-1389, CVE-2020-1426. **CVE ID : CVE-2020-1419**		
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists when Windows Error Reporting improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Error Reporting Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1420**	N/A	O-MIC-WIND-100820/1826
Access of Resource Using Incompatible Type ('Type Confusion')	7/14/2020	9.3	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1421**	N/A	O-MIC-WIND-100820/1827
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'.	N/A	O-MIC-WIND-100820/1828

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This CVE ID is unique from CVE-2020-1249, CVE-2020-1353, CVE-2020-1370, CVE-2020-1399, CVE-2020-1404, CVE-2020-1413, CVE-2020-1414, CVE-2020-1415. **CVE ID : CVE-2020-1422**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Subsystem for Linux handles files, aka 'Windows Subsystem for Linux Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1423**	N/A	O-MIC-WIND-100820/1829
Improper Privilege Management	7/14/2020	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'. **CVE ID : CVE-2020-1424**	N/A	O-MIC-WIND-100820/1830
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1367, CVE-2020-1389, CVE-2020-1419. **CVE ID : CVE-2020-1426**	N/A	O-MIC-WIND-100820/1831

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1390, CVE-2020-1428, CVE-2020-1438. **CVE ID : CVE-2020-1427**	N/A	O-MIC-WIND-100820/1832
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1390, CVE-2020-1427, CVE-2020-1438. **CVE ID : CVE-2020-1428**	N/A	O-MIC-WIND-100820/1833
Improper Privilege Management	7/14/2020	7.2	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles a process crash, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1429**	N/A	O-MIC-WIND-100820/1834
Improper	7/14/2020	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 UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows UPnP Device Host Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1354. **CVE ID : CVE-2020-1430**		100820/1835
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows AppX Deployment Extensions improperly performs privilege management, resulting in access to system files.To exploit this vulnerability, an authenticated attacker would need to run a specially crafted application to elevate privileges.The security update addresses the vulnerability by correcting how AppX Deployment Extensions manages privileges., aka 'Windows AppX Deployment Extensions Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1431**	N/A	O-MIC-WIND-100820/1836
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists when Skype for Business is	N/A	O-MIC-WIND-100820/1837

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			accessed via Internet Explorer, aka 'Skype for Business via Internet Explorer Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1432**		
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists when Microsoft Edge PDF Reader improperly handles objects in memory, aka 'Microsoft Edge PDF Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1433**	N/A	O-MIC-WIND-100820/1838
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Sync Host Service handles objects in memory, aka 'Windows Sync Host Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1434**	N/A	O-MIC-WIND-100820/1839
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	9.3	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1435**	N/A	O-MIC-WIND-100820/1840
Improper Input Validation	7/14/2020	6.8	A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted fonts.For all systems except	N/A	O-MIC-WIND-100820/1841

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Windows 10, an attacker who successfully exploited the vulnerability could execute code remotely, aka 'Windows Font Library Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1436**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Location Awareness Service handles objects in memory, aka 'Windows Network Location Awareness Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1437**	N/A	O-MIC-WIND-100820/1842
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1390, CVE-2020-1427, CVE-2020-1428. **CVE ID : CVE-2020-1438**	N/A	O-MIC-WIND-100820/1843
Improper Privilege Management	7/14/2020	3.6	An elevation of privilege vulnerability exists when the MpSigStub.exe for Defender allows file deletion in arbitrary locations.To exploit the	N/A	O-MIC-WIND-100820/1844

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Defender Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1461**		
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists when Skype for Business is accessed via Microsoft Edge (EdgeHTML-based), aka 'Skype for Business via Microsoft Edge (EdgeHTML-based) Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1462**	N/A	O-MIC-WIND-100820/1845
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the SharedStream Library handles objects in memory, aka 'Windows SharedStream Library Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1463**	N/A	O-MIC-WIND-100820/1846
Information Exposure	7/14/2020	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'. **CVE ID : CVE-2020-1468**	N/A	O-MIC-WIND-100820/1847
windows_server_2019					
Improper	7/14/2020	4.6	An elevation of privilege	N/A	O-MIC-WIND-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1085**		100820/1848
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1427, CVE-2020-1428, CVE-2020-1438. **CVE ID : CVE-2020-1390**	N/A	O-MIC-WIND-100820/1849
N/A	7/14/2020	6.8	A remote code execution vulnerability exists in .NET Framework, Microsoft SharePoint, and Visual Studio when the software fails to check the source markup of XML file input, aka '.NET Framework, SharePoint Server, and Visual Studio Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1147**	N/A	O-MIC-WIND-100820/1850
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects	N/A	O-MIC-WIND-100820/1851

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1353, CVE-2020-1370, CVE-2020-1399, CVE-2020-1404, CVE-2020-1413, CVE-2020-1414, CVE-2020-1415, CVE-2020-1422. **CVE ID : CVE-2020-1249**		
Improper Input Validation	7/14/2020	4	This security update corrects a denial of service in the Local Security Authority Subsystem Service (LSASS) caused when an authenticated attacker sends a specially crafted authentication request, aka 'Local Security Authority Subsystem Service Denial of Service Vulnerability'. **CVE ID : CVE-2020-1267**	N/A	O-MIC-WIND-100820/1852
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists when Windows Mobile Device Management (MDM) Diagnostics improperly handles junctions, aka 'Windows Mobile Device Management Diagnostics Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1330**	N/A	O-MIC-WIND-100820/1853
Improper Privilege Management	7/14/2020	3.7	An elevation of privilege vulnerability exists when Group Policy Services Policy Processing	N/A	O-MIC-WIND-100820/1854

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improperly handle reparse points, aka 'Group Policy Services Policy Processing Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1333**		
Improper Privilege Management	7/14/2020	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-2020-1411. **CVE ID : CVE-2020-1336**	N/A	O-MIC-WIND-100820/1855
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows WalletService handles objects in memory, aka 'Windows WalletService Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1362, CVE-2020-1369. **CVE ID : CVE-2020-1344**	N/A	O-MIC-WIND-100820/1856
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Modules Installer improperly handles file operations, aka 'Windows Modules Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1346**	N/A	O-MIC-WIND-100820/1857
Improper Privilege	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Storage	N/A	O-MIC-WIND-100820/1858

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Services improperly handle file operations, aka 'Windows Storage Services Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1347**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	10	A remote code execution vulnerability exists in Windows Domain Name System servers when they fail to properly handle requests, aka 'Windows DNS Server Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1350**	N/A	O-MIC-WIND-100820/1859
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists when the Windows Graphics component improperly handles objects in memory, aka 'Microsoft Graphics Component Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1351**	N/A	O-MIC-WIND-100820/1860
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows USO Core Worker improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows USO Core Worker Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1352**	N/A	O-MIC-WIND-100820/1861

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	7/14/2020	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-2020-1249, CVE-2020-1370, CVE-2020-1399, CVE-2020-1404, CVE-2020-1413, CVE-2020-1414, CVE-2020-1415, CVE-2020-1422. **CVE ID : CVE-2020-1353**	N/A	O-MIC-WIND-100820/1862
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows UPnP Device Host Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1430. **CVE ID : CVE-2020-1354**	N/A	O-MIC-WIND-100820/1863
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows iSCSI Target Service improperly handles file operations, aka 'Windows iSCSI Target Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1356**	N/A	O-MIC-WIND-100820/1864

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows System Events Broker improperly handles file operations, aka 'Windows System Events Broker Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1357**	N/A	O-MIC-WIND-100820/1865
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists when the Windows Resource Policy component improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Resource Policy Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1358**	N/A	O-MIC-WIND-100820/1866
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Cryptography Next Generation (CNG) Key Isolation service improperly handles memory, aka 'Windows CNG Key Isolation Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1384. **CVE ID : CVE-2020-1359**	N/A	O-MIC-WIND-100820/1867
Improper Privilege	7/14/2020	4.6	An elevation of privilege vulnerability exists when	N/A	O-MIC-WIND-100820/1868

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			the Windows Profile Service improperly handles file operations, aka 'Windows Profile Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1360**		
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists in the way that the WalletService handles memory.To exploit the vulnerability, an attacker would first need code execution on a victim system, aka 'Windows WalletService Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1361**	N/A	O-MIC-WIND-100820/1869
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows WalletService handles objects in memory, aka 'Windows WalletService Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1344, CVE-2020-1369. **CVE ID : CVE-2020-1362**	N/A	O-MIC-WIND-100820/1870
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Picker Platform improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Picker Platform	N/A	O-MIC-WIND-100820/1871

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1363**		
Improper Input Validation	7/14/2020	3.6	A denial of service vulnerability exists in the way that the WalletService handles files, aka 'Windows WalletService Denial of Service Vulnerability'. **CVE ID : CVE-2020-1364**	N/A	O-MIC-WIND-100820/1872
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Event Logging Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Event Logging Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1371. **CVE ID : CVE-2020-1365**	N/A	O-MIC-WIND-100820/1873
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Print Workflow Service improperly handles objects in memory, aka 'Windows Print Workflow Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1366**	N/A	O-MIC-WIND-100820/1874
Information	7/14/2020	2.1	An information disclosure vulnerability exists when	N/A	O-MIC-WIND-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1389, CVE-2020-1419, CVE-2020-1426. **CVE ID : CVE-2020-1367**		100820/1875
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Credential Enrollment Manager service handles objects in memory, aka 'Windows Credential Enrollment Manager Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1368**	N/A	O-MIC-WIND-100820/1876
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows WalletService handles objects in memory, aka 'Windows WalletService Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1344, CVE-2020-1362. **CVE ID : CVE-2020-1369**	N/A	O-MIC-WIND-100820/1877
Improper Privilege Management	7/14/2020	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	N/A	O-MIC-WIND-100820/1878

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-1249, CVE-2020-1353, CVE-2020-1399, CVE-2020-1404, CVE-2020-1413, CVE-2020-1414, CVE-2020-1415, CVE-2020-1422. **CVE ID : CVE-2020-1370**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Event Logging Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Event Logging Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1365. **CVE ID : CVE-2020-1371**	N/A	O-MIC-WIND-100820/1879
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when Windows Mobile Device Management (MDM) Diagnostics improperly handles objects in memory, aka 'Windows Mobile Device Management Diagnostics Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1405. **CVE ID : CVE-2020-1372**	N/A	O-MIC-WIND-100820/1880
Improper Privilege	7/14/2020	4.6	An elevation of privilege vulnerability exists in the	N/A	O-MIC-WIND-100820/1881

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1390, CVE-2020-1427, CVE-2020-1428, CVE-2020-1438. **CVE ID : CVE-2020-1373**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	5.1	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1374**	N/A	O-MIC-WIND-100820/1882
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when Windows improperly handles COM object creation, aka 'Windows COM Server Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1375**	N/A	O-MIC-WIND-100820/1883
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Cryptography Next Generation (CNG) Key Isolation service improperly handles memory, aka 'Windows CNG Key Isolation Service	N/A	O-MIC-WIND-100820/1884

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1359. **CVE ID : CVE-2020-1384**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Credential Picker handles objects in memory, aka 'Windows Credential Picker Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1385**	N/A	O-MIC-WIND-100820/1885
Information Exposure	7/14/2020	2.1	An information vulnerability exists when Windows Connected User Experiences and Telemetry Service improperly discloses file information, aka 'Connected User Experiences and Telemetry Service Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1386**	N/A	O-MIC-WIND-100820/1886
Improper Privilege Management	7/14/2020	4.6	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-2020-1387**	N/A	O-MIC-WIND-100820/1887
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the psmsrv.dll handles objects in	N/A	O-MIC-WIND-100820/1888

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1392, CVE-2020-1394, CVE-2020-1395. **CVE ID : CVE-2020-1388**		
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1367, CVE-2020-1419, CVE-2020-1426. **CVE ID : CVE-2020-1389**	N/A	O-MIC-WIND-100820/1889
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Delivery Optimization service improperly handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1388, CVE-2020-1394, CVE-2020-1395. **CVE ID : CVE-2020-1392**	N/A	O-MIC-WIND-100820/1890
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows Diagnostics Hub Standard Collector Service fails to properly sanitize input, leading to an unsecure library-loading behavior, aka	N/A	O-MIC-WIND-100820/1891

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			'Windows Diagnostics Hub Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1418. **CVE ID : CVE-2020-1393**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Geolocation Framework handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1388, CVE-2020-1392, CVE-2020-1395. **CVE ID : CVE-2020-1394**	N/A	O-MIC-WIND-100820/1892
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Speech Brokered API handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1388, CVE-2020-1392, CVE-2020-1394. **CVE ID : CVE-2020-1395**	N/A	O-MIC-WIND-100820/1893
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to Advanced Local Procedure Call (ALPC).An attacker who successfully exploited this vulnerability could run arbitrary code in the	N/A	O-MIC-WIND-100820/1894

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			security context of the local system, aka 'Windows ALPC Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1396**		
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists in Windows when the Windows Imaging Component fails to properly handle objects in memory, aka 'Windows Imaging Component Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1397**	N/A	O-MIC-WIND-100820/1895
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when Windows Lockscreen fails to properly handle Ease of Access dialog.An attacker who successfully exploited the vulnerability could execute commands with elevated permissions.The security update addresses the vulnerability by ensuring that the Ease of Access dialog is handled properly., aka 'Windows Lockscreen Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1398**	N/A	O-MIC-WIND-100820/1896
Improper Privilege Management	7/14/2020	4.6	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-100820/1897

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1249, CVE-2020-1353, CVE-2020-1370, CVE-2020-1404, CVE-2020-1413, CVE-2020-1414, CVE-2020-1415, CVE-2020-1422. **CVE ID : CVE-2020-1399**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	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-2020-1401, CVE-2020-1407. **CVE ID : CVE-2020-1400**	N/A	O-MIC-WIND-100820/1898
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	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-2020-1400, CVE-2020-1407. **CVE ID : CVE-2020-1401**	N/A	O-MIC-WIND-100820/1899
Improper Privilege Management	7/14/2020	7.2	An elevation of privilege vulnerability exists when the Windows ActiveX Installer Service improperly handles memory.To exploit this vulnerability, an attacker would first have to gain	N/A	O-MIC-WIND-100820/1900

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution on the victim system, aka 'Windows ActiveX Installer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1402**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	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'. **CVE ID : CVE-2020-1403**	N/A	O-MIC-WIND-100820/1901
Improper Privilege Management	7/14/2020	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-2020-1249, CVE-2020-1353, CVE-2020-1370, CVE-2020-1399, CVE-2020-1413, CVE-2020-1414, CVE-2020-1415, CVE-2020-1422. **CVE ID : CVE-2020-1404**	N/A	O-MIC-WIND-100820/1902
Improper Privilege Management	7/14/2020	3.6	An elevation of privilege vulnerability exists when Windows Mobile Device Management (MDM) Diagnostics improperly handles junctions, aka 'Windows Mobile Device Management Diagnostics Elevation of Privilege Vulnerability'. This CVE ID	N/A	O-MIC-WIND-100820/1903

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is unique from CVE-2020-1372. **CVE ID : CVE-2020-1405**		
Improper Privilege Management	7/14/2020	7.2	An elevation of privilege vulnerability exists in the way that the Windows Network List Service handles objects in memory, aka 'Windows Network List Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1406**	N/A	O-MIC-WIND-100820/1904
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	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-2020-1400, CVE-2020-1401. **CVE ID : CVE-2020-1407**	N/A	O-MIC-WIND-100820/1905
Origin Validation Error	7/14/2020	9.3	A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Microsoft Graphics Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1408**	N/A	O-MIC-WIND-100820/1906
Improper Restriction of Operations within the Bounds of a	7/14/2020	9.3	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite	N/A	O-MIC-WIND-100820/1907

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1409**		
N/A	7/14/2020	9.3	A remote code execution vulnerability exists when Windows Address Book (WAB) improperly processes vcard files.To exploit the vulnerability, an attacker could send a malicious vcard that a victim opens using Windows Address Book (WAB), aka 'Windows Address Book Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1410**	N/A	O-MIC-WIND-100820/1908
Improper Privilege Management	7/14/2020	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-2020-1336. **CVE ID : CVE-2020-1411**	N/A	O-MIC-WIND-100820/1909
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	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-2020-1412**	N/A	O-MIC-WIND-100820/1910
Improper Privilege	7/14/2020	4.6	An elevation of privilege vulnerability exists when	N/A	O-MIC-WIND-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			the Windows Runtime improperly handles objects in memory, aka 'Windows Runtime Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1249, CVE-2020-1353, CVE-2020-1370, CVE-2020-1399, CVE-2020-1404, CVE-2020-1414, CVE-2020-1415, CVE-2020-1422. **CVE ID : CVE-2020-1413**		100820/1911
Improper Privilege Management	7/14/2020	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-2020-1249, CVE-2020-1353, CVE-2020-1370, CVE-2020-1399, CVE-2020-1404, CVE-2020-1413, CVE-2020-1415, CVE-2020-1422. **CVE ID : CVE-2020-1414**	N/A	O-MIC-WIND-100820/1912
Improper Privilege Management	7/14/2020	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-2020-1249, CVE-2020-1353, CVE-2020-1370, CVE-2020-1399, CVE-2020-1404, CVE-	N/A	O-MIC-WIND-100820/1913

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-1413, CVE-2020-1414, CVE-2020-1422. **CVE ID : CVE-2020-1415**		
Improper Privilege Management	7/14/2020	9.3	An elevation of privilege vulnerability exists in Visual Studio and Visual Studio Code when they load software dependencies, aka 'Visual Studio and Visual Studio Code Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1416**	N/A	O-MIC-WIND-100820/1914
Improper Input Validation	7/14/2020	7.2	An elevation of privilege vulnerability exists when the Windows Diagnostics Execution Service fails to properly sanitize input, leading to an unsecure library-loading behavior, aka 'Windows Diagnostics Hub Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1393. **CVE ID : CVE-2020-1418**	N/A	O-MIC-WIND-100820/1915
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	2.1	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1367, CVE-2020-1389, CVE-2020-1426. **CVE ID : CVE-2020-1419**	N/A	O-MIC-WIND-100820/1916

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists when Windows Error Reporting improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Error Reporting Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1420**	N/A	O-MIC-WIND-100820/1917
Access of Resource Using Incompatible Type ('Type Confusion')	7/14/2020	9.3	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1421**	N/A	O-MIC-WIND-100820/1918
Improper Privilege Management	7/14/2020	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-2020-1249, CVE-2020-1353, CVE-2020-1370, CVE-2020-1399, CVE-2020-1404, CVE-2020-1413, CVE-2020-1414, CVE-2020-1415.	N/A	O-MIC-WIND-110820/1919

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1422		
Improper Privilege Management	7/14/2020	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'. **CVE ID : CVE-2020-1424**	N/A	O-MIC-WIND-110820/1920
Information Exposure	7/14/2020	2.1	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-1367, CVE-2020-1389, CVE-2020-1419. **CVE ID : CVE-2020-1426**	N/A	O-MIC-WIND-110820/1921
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1390, CVE-2020-1428, CVE-2020-1438. **CVE ID : CVE-2020-1427**	N/A	O-MIC-WIND-110820/1922
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows	N/A	O-MIC-WIND-110820/1923

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1390, CVE-2020-1427, CVE-2020-1438. **CVE ID : CVE-2020-1428**		
Improper Privilege Management	7/14/2020	7.2	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles a process crash, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1429**	N/A	O-MIC-WIND-110820/1924
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows UPnP Device Host improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows UPnP Device Host Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1354. **CVE ID : CVE-2020-1430**	N/A	O-MIC-WIND-110820/1925
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists when the Windows AppX	N/A	O-MIC-WIND-110820/1926

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Deployment Extensions improperly performs privilege management, resulting in access to system files.To exploit this vulnerability, an authenticated attacker would need to run a specially crafted application to elevate privileges.The security update addresses the vulnerability by correcting how AppX Deployment Extensions manages privileges., aka 'Windows AppX Deployment Extensions Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1431**		
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists when Skype for Business is accessed via Internet Explorer, aka 'Skype for Business via Internet Explorer Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1432**	N/A	O-MIC-WIND-110820/1927
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists when Microsoft Edge PDF Reader improperly handles objects in memory, aka 'Microsoft Edge PDF Information Disclosure Vulnerability'. **CVE ID : CVE-2020-1433**	N/A	O-MIC-WIND-110820/1928
Improper	7/14/2020	4.6	An elevation of privilege	N/A	O-MIC-WIND-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			vulnerability exists in the way that the Windows Sync Host Service handles objects in memory, aka 'Windows Sync Host Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1434**		110820/1929
Improper Restriction of Operations within the Bounds of a Memory Buffer	7/14/2020	9.3	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1435**	N/A	O-MIC-WIND-110820/1930
Improper Input Validation	7/14/2020	6.8	A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted fonts.For all systems except Windows 10, an attacker who successfully exploited the vulnerability could execute code remotely, aka 'Windows Font Library Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-1436**	N/A	O-MIC-WIND-110820/1931
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Location Awareness Service handles objects in memory, aka 'Windows Network Location Awareness	N/A	O-MIC-WIND-110820/1932

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1437**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the Windows Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1373, CVE-2020-1390, CVE-2020-1427, CVE-2020-1428. **CVE ID : CVE-2020-1438**	N/A	O-MIC-WIND-110820/1933
Improper Privilege Management	7/14/2020	3.6	An elevation of privilege vulnerability exists when the MpSigStub.exe for Defender allows file deletion in arbitrary locations.To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Defender Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1461**	N/A	O-MIC-WIND-110820/1934
Information Exposure	7/14/2020	4.3	An information disclosure vulnerability exists when Skype for Business is accessed via Microsoft Edge (EdgeHTML-based), aka 'Skype for Business via Microsoft Edge (EdgeHTML-based) Information Disclosure	N/A	O-MIC-WIND-110820/1935

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. **CVE ID : CVE-2020-1462**		
Improper Privilege Management	7/14/2020	4.6	An elevation of privilege vulnerability exists in the way that the SharedStream Library handles objects in memory, aka 'Windows SharedStream Library Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-1463**	N/A	O-MIC-WIND-110820/1936
Information Exposure	7/14/2020	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'. **CVE ID : CVE-2020-1468**	N/A	O-MIC-WIND-110820/1937
azure_devops_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/14/2020	3.5	A Cross-site Scripting (XSS) vulnerability exists when Azure DevOps Server does not properly sanitize user provided input, aka 'Azure DevOps Server Cross-site Scripting Vulnerability'. **CVE ID : CVE-2020-1326**	N/A	O-MIC-AZUR-110820/1938
Mitsubishielectric					
coreos					
Buffer Copy without Checking Size of Input ('Classic Buffer	7/7/2020	7.5	TCP/IP function included in the firmware of Mitsubishi Electric GOT2000 series (CoreOS with version -Y and earlier installed in GT27 Model,	N/A	O-MIT-CORE-110820/1939

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			GT25 Model, and GT23 Model) contains a buffer overflow vulnerability, which may allow a remote attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet. **CVE ID : CVE-2020-5595**		
Session Fixation	7/7/2020	5	TCP/IP function included in the firmware of Mitsubishi Electric GOT2000 series (CoreOS with version -Y and earlier installed in GT27 Model, GT25 Model, and GT23 Model) does not properly manage sessions, which may allow a remote attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet. **CVE ID : CVE-2020-5596**	N/A	O-MIT-CORE-110820/1940
NULL Pointer Dereference	7/7/2020	5	TCP/IP function included in the firmware of Mitsubishi Electric GOT2000 series (CoreOS with version -Y and earlier installed in GT27 Model, GT25 Model, and GT23 Model) contains a null pointer dereference vulnerability, which may allow a remote attacker to stop the network functions of the products or execute a malicious program via a	N/A	O-MIT-CORE-110820/1941

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specially crafted packet. **CVE ID : CVE-2020-5597**		
Incorrect Authorization	7/7/2020	5	TCP/IP function included in the firmware of Mitsubishi Electric GOT2000 series (CoreOS with version -Y and earlier installed in GT27 Model, GT25 Model, and GT23 Model) contains an improper access control vulnerability, which may which may allow a remote attacker tobypass access restriction and stop the network functions of the products or execute a malicious program via a specially crafted packet. **CVE ID : CVE-2020-5598**	N/A	O-MIT-CORE-110820/1942
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	7/7/2020	10	TCP/IP function included in the firmware of Mitsubishi Electric GOT2000 series (CoreOS with version -Y and earlier installed in GT27 Model, GT25 Model, and GT23 Model) contains an improper neutralization of argument delimiters in a command ('Argument Injection') vulnerability, which may allow a remote attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet. **CVE ID : CVE-2020-5599**	N/A	O-MIT-CORE-110820/1943

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	7/7/2020	5	TCP/IP function included in the firmware of Mitsubishi Electric GOT2000 series (CoreOS with version -Y and earlier installed in GT27 Model, GT25 Model, and GT23 Model) contains a resource management error vulnerability, which may allow a remote attacker to stop the network functions of the products or execute a malicious program via a specially crafted packet. **CVE ID : CVE-2020-5600**	N/A	O-MIT-CORE-110820/1944
Moxa					
edr-g902-t_firmware					
Out-of-bounds Write	7/15/2020	7.5	Malicious operation of the crafted web browser cookie may cause a stack-based buffer overflow in the system web server on the EDR-G902 and EDR-G903 Series Routers (versions prior to 5.4). **CVE ID : CVE-2020-14511**	N/A	O-MOX-EDR--110820/1945
edr-g902_firmware					
Out-of-bounds Write	7/15/2020	7.5	Malicious operation of the crafted web browser cookie may cause a stack-based buffer overflow in the system web server on the EDR-G902 and EDR-G903 Series Routers (versions prior to 5.4). **CVE ID : CVE-2020-14511**	N/A	O-MOX-EDR--110820/1946
edr-g903-t_firmware					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	7/15/2020	7.5	Malicious operation of the crafted web browser cookie may cause a stack-based buffer overflow in the system web server on the EDR-G902 and EDR-G903 Series Routers (versions prior to 5.4). **CVE ID : CVE-2020-14511**	N/A	O-MOX-EDR--110820/1947
edr-g903_firmware					
Out-of-bounds Write	7/15/2020	7.5	Malicious operation of the crafted web browser cookie may cause a stack-based buffer overflow in the system web server on the EDR-G902 and EDR-G903 Series Routers (versions prior to 5.4). **CVE ID : CVE-2020-14511**	N/A	O-MOX-EDR--110820/1948
Opensuse					
leap					
Use of a Broken or Risky Cryptographic Algorithm	7/9/2020	1.2	During RSA key generation, bignum implementations used a variation of the Binary Extended Euclidean Algorithm which entailed significantly input-dependent flow. This allowed an attacker able to perform electromagnetic-based side channel attacks to record traces leading to the recovery of the secret primes. *Note:* An unmodified Firefox browser does not generate RSA keys in normal operation and is not	N/A	O-OPE-LEAP-110820/1949

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected, but products built on top of it might. This vulnerability affects Firefox < 78. **CVE ID : CVE-2020-12402**		
NULL Pointer Dereference	7/7/2020	4	A NULL pointer dereference, or possible use-after-free flaw was found in Samba AD LDAP server in versions before 4.10.17, before 4.11.11 and before 4.12.4. Although some versions of Samba shipped with Red Hat Enterprise Linux do not support Samba in AD mode, the affected code is shipped with the libldb package. This flaw allows an authenticated user to possibly trigger a use-after-free or NULL pointer dereference. The highest threat from this vulnerability is to system availability. **CVE ID : CVE-2020-10730**	N/A	O-OPE-LEAP-110820/1950
Uncontrolled Resource Consumption	7/7/2020	7.8	A flaw was found in all Samba versions before 4.10.17, before 4.11.11 and before 4.12.4 in the way it processed NetBios over TCP/IP. This flaw allows a remote attacker could to cause the Samba server to consume excessive CPU use, resulting in a denial of service. This highest threat from this vulnerability is to system availability.	N/A	O-OPE-LEAP-110820/1951

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-10745		
Out-of-bounds Read	7/9/2020	2.1	An out-of-bounds read vulnerability was found in the SLiRP networking implementation of the QEMU emulator. This flaw occurs in the icmp6_send_echoreply() routine while replying to an ICMP echo request, also known as ping. This flaw allows a malicious guest to leak the contents of the host memory, resulting in possible information disclosure. This flaw affects versions of libslirp before 4.3.1. **CVE ID : CVE-2020-10756**	N/A	O-OPE-LEAP-110820/1952
Use After Free	7/6/2020	4	A use-after-free flaw was found in all samba LDAP server versions before 4.10.17, before 4.11.11, before 4.12.4 used in a AC DC configuration. A Samba LDAP user could use this flaw to crash samba. **CVE ID : CVE-2020-10760**	N/A	O-OPE-LEAP-110820/1953
Improper Input Validation	7/6/2020	5	A flaw was found in the AD DC NBT server in all Samba versions before 4.10.17, before 4.11.11 and before 4.12.4. A samba user could send an empty UDP packet to cause the samba server to crash. **CVE ID : CVE-2020-14303**	https://security.netapp.com/advisory/ntap-20200709-0003/	O-OPE-LEAP-110820/1954
Oracle					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
solaris					
Improper Resource Shutdown or Release	7/15/2020	4.7	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Packaging Scripts). The supported version that is affected is 11. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Solaris, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:C/C:N/I:N/A:H). **CVE ID : CVE-2020-14537**	N/A	O-ORA-SOLA-110820/1955
Information Exposure	7/15/2020	2.1	Vulnerability in the Oracle Solaris product of Oracle Systems (component: libsuri). The supported version that is affected is 11. Easily exploitable vulnerability allows low	N/A	O-ORA-SOLA-110820/1956

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Solaris accessible data. CVSS 3.1 Base Score 3.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2020-14542**		
N/A	7/15/2020	3.3	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Device Driver Utility). The supported version that is affected is 11. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Solaris accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Solaris. CVSS 3.1	N/A	O-ORA-SOLA-110820/1957

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Base Score 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:N/I:H/A:L). **CVE ID : CVE-2020-14545**		
N/A	7/15/2020	4.4	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Device Driver Utility). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Solaris. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2020-14724**	N/A	O-ORA-SOLA-110820/1958
Paloaltonetworks					
pan-os					
Inadequate Encryption Strength	7/8/2020	5.8	Certain communication between PAN-OS and cloud-delivered services inadvertently use TLS 1.0, which is known to be a cryptographically weak	N/A	O-PAL-PAN--110820/1959

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protocol. These cloud services include Cortex Data Lake, the Customer Support Portal, and the Prisma Access infrastructure. Conditions required for exploitation of known TLS 1.0 weaknesses do not exist for the communication between PAN-OS and cloud-delivered services. We do not believe that any communication is impacted as a result of known attacks against TLS 1.0. This issue impacts: All versions of PAN-OS 8.0; PAN-OS 8.1 versions earlier than PAN-OS 8.1.14; PAN-OS 9.0 versions earlier than PAN-OS 9.0.9; PAN-OS 9.1 versions earlier than PAN-OS 9.1.3. PAN-OS 7.1 is not impacted by this issue. **CVE ID : CVE-2020-1982**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	7/8/2020	9	An OS Command Injection vulnerability in the PAN-OS management interface that allows authenticated administrators to execute arbitrary OS commands with root privileges. This issue impacts PAN-OS 8.1 versions earlier than PAN-OS 8.1.15; and all versions of PAN-OS 7.1 and PAN-OS 8.0. This issue does not impact PAN-OS 9.0, PAN-OS 9.1, or Prisma Access	N/A	O-PAL-PAN--110820/1960

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			services. **CVE ID : CVE-2020-2030**		
Integer Underflow (Wrap or Wraparound)	7/8/2020	6.8	An integer underflow vulnerability in the dnsproxyd component of the PAN-OS management interface allows authenticated administrators to issue a command from the command line interface that causes the component to stop responding. Repeated attempts to send this request result in denial of service to all PAN-OS services by restarting the device and putting it into maintenance mode. This issue impacts: PAN-OS 9.1 versions earlier than PAN-OS 9.1.3. This issue does not impact PAN-OS 8.1, PAN-OS 9.0, or Prisma Access services. **CVE ID : CVE-2020-2031**	N/A	O-PAL-PAN--110820/1961
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	7/8/2020	9.3	An OS Command Injection vulnerability in the PAN-OS GlobalProtect portal allows an unauthenticated network based attacker to execute arbitrary OS commands with root privileges. An attacker requires some knowledge of the firewall to exploit this issue. This issue can not be exploited if GlobalProtect portal feature is not enabled. This	N/A	O-PAL-PAN--110820/1962

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue impacts PAN-OS 9.1 versions earlier than PAN-OS 9.1.3; PAN-OS 8.1 versions earlier than PAN-OS 8.1.15; PAN-OS 9.0 versions earlier than PAN-OS 9.0.9; all versions of PAN-OS 8.0 and PAN-OS 7.1. Prisma Access services are not impacted by this vulnerability. **CVE ID : CVE-2020-2034**		
Realtek					
rtl8711am_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/6/2020	4.9	An issue was discovered on Realtek RTL8195AM, RTL8711AM, RTL8711AF, and RTL8710AF devices before 2.0.6. A stack-based buffer overflow exists in the client code that takes care of WPA2's 4-way-handshake via a malformed EAPOL-Key packet with a long keydata buffer. **CVE ID : CVE-2020-9395**	N/A	O-REA-RTL8-110820/1963
rtl8195am_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/6/2020	4.9	An issue was discovered on Realtek RTL8195AM, RTL8711AM, RTL8711AF, and RTL8710AF devices before 2.0.6. A stack-based buffer overflow exists in the client code that takes care of WPA2's 4-way-handshake via a malformed EAPOL-Key packet with a long keydata	N/A	O-REA-RTL8-110820/1964

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			buffer. **CVE ID : CVE-2020-9395**		
rtl8710af_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/6/2020	4.9	An issue was discovered on Realtek RTL8195AM, RTL8711AM, RTL8711AF, and RTL8710AF devices before 2.0.6. A stack-based buffer overflow exists in the client code that takes care of WPA2's 4-way-handshake via a malformed EAPOL-Key packet with a long keydata buffer. **CVE ID : CVE-2020-9395**	N/A	O-REA-RTL8-110820/1965
rtl8711af_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/6/2020	4.9	An issue was discovered on Realtek RTL8195AM, RTL8711AM, RTL8711AF, and RTL8710AF devices before 2.0.6. A stack-based buffer overflow exists in the client code that takes care of WPA2's 4-way-handshake via a malformed EAPOL-Key packet with a long keydata buffer. **CVE ID : CVE-2020-9395**	N/A	O-REA-RTL8-110820/1966
Redhat					
enterprise_linux_server					
Improper Check for Dropped Privileges	7/13/2020	4.6	The version of docker as released for Red Hat Enterprise Linux 7 Extras via RHBA-2020:0053 advisory included an incorrect version of runc	https://access.redhat.com/errata/RHBA-2020:0427, https://acc	O-RED-ENTE-110820/1967

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			missing the fix for CVE-2019-5736, which was previously fixed via RHSA-2019:0304. This issue could allow a malicious or compromised container to compromise the container host and other containers running on the same host. This issue only affects docker version 1.13.1-108.git4ef4b30.el7, shipped in Red Hat Enterprise Linux 7 Extras. Both earlier and later versions are not affected. **CVE ID : CVE-2020-14298**	ess.redhat.com/security/cve/CVE-2020-14298, https://access.redhat.com/security/vulnerabilities/runcescape, https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-5736	
Improper Check for Dropped Privileges	7/13/2020	4.6	The docker packages version docker-1.13.1-108.git4ef4b30.el7 as released for Red Hat Enterprise Linux 7 Extras via RHBA-2020:0053 (https://access.redhat.com/errata/RHBA-2020:0053) included an incorrect version of runc that was missing multiple bug and security fixes. One of the fixes regressed in that update was the fix for CVE-2016-9962, that was previously corrected in the docker packages in Red Hat Enterprise Linux 7 Extras via RHSA-2017:0116 (https://access.redhat.com/errata/RHSA-2017:0116). The CVE-2020-14300 was assigned to this security	https://access.redhat.com/errata/RHBA-2020:0427, https://access.redhat.com/security/cve/CVE-2016-9962, https://access.redhat.com/security/vulnerabilities/cve-2016-9962, https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2016-9962	O-RED-ENTE-110820/1968

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			regression and it is specific to the docker packages produced by Red Hat. The original issue - CVE-2016-9962 - could possibly allow a process inside container to compromise a process entering container namespace and execute arbitrary code outside of the container. This could lead to compromise of the container host or other containers running on the same container host. This issue only affects a single version of Docker, 1.13.1-108.git4ef4b30, shipped in Red Hat Enterprise Linux 7. Both earlier and later versions are not affected. **CVE ID : CVE-2020-14300**		
enterprise_linux					
Out-of-bounds Read	7/9/2020	2.1	An out-of-bounds read vulnerability was found in the SLiRP networking implementation of the QEMU emulator. This flaw occurs in the icmp6_send_echoreply() routine while replying to an ICMP echo request, also known as ping. This flaw allows a malicious guest to leak the contents of the host memory, resulting in possible information disclosure. This flaw affects versions of libslirp before 4.3.1.	N/A	O-RED-ENTE-110820/1969

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		🟩	**CVE ID : CVE-2020-10756**		
Improper Certificate Validation	7/14/2020	4	libldap in certain third-party OpenLDAP packages has a certificate-validation flaw when the third-party package is asserting RFC6125 support. It considers CN even when there is a non-matching subjectAltName (SAN). This is fixed in, for example, openldap-2.4.46-10.el8 in Red Hat Enterprise Linux. **CVE ID : CVE-2020-15719**	N/A	O-RED-ENTE-110820/1970
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/8/2020	4.3	A security vulnerability in HPE IceWall SSO Dfw and Dgfw (Domain Gateway Option) could be exploited remotely to cause a remote cross-site scripting (XSS). HPE has provided the following information to resolve this vulnerability in HPE IceWall SSO DFW and Dgfw: https://www.hpe.com/jp/icewall_patchaccess **CVE ID : CVE-2020-7140**	N/A	O-RED-ENTE-110820/1971
riot-os					
riot					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/7/2020	7.5	RIOT 2020.04 has a buffer overflow in the base64 decoder. The decoding function base64_decode() uses an output buffer estimation function to compute the required buffer capacity and	N/A	O-RIO-RIOT-110820/1972

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validate against the provided buffer size. The base64_estimate_decode_size() function calculates the expected decoded size with an arithmetic round-off error and does not take into account possible padding bytes. Due to this underestimation, it may be possible to craft base64 input that causes a buffer overflow. **CVE ID : CVE-2020-15350**		
rittal					
cmciii-pu-9333e0fb_firmware					
Use of Hard-coded Credentials	7/14/2020	10	An issue was discovered on Rittal PDU-3C002DEC through 5.17.10 and CMCIII-PU-9333E0FB through 3.17.10 devices. There is a Backdoor root account. **CVE ID : CVE-2020-11951**	N/A	O-RIT-CMCI-110820/1973
Information Exposure	7/14/2020	4.9	An issue was discovered on Rittal PDU-3C002DEC through 5.17.10 and CMCIII-PU-9333E0FB through 3.17.10 devices. Attackers can bypass the CLI menu. **CVE ID : CVE-2020-11952**	N/A	O-RIT-CMCI-110820/1974
Improper Neutralization of Special Elements used in an OS Command ('OS Command	7/14/2020	9	An issue was discovered on Rittal PDU-3C002DEC through 5.15.40 and CMCIII-PU-9333E0FB through 3.15.70_4 devices. Attackers can execute	N/A	O-RIT-CMCI-110820/1975

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			code. **CVE ID : CVE-2020-11953**		
Incorrect Default Permissions	7/14/2020	9	An issue was discovered on Rittal PDU-3C002DEC through 5.15.70 and CMCIII-PU-9333E0FB through 3.15.70 devices. There are insecure permissions. **CVE ID : CVE-2020-11955**	N/A	O-RIT-CMCI-110820/1976
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	7/14/2020	10	An issue was discovered on Rittal PDU-3C002DEC through 5.17.10 and CMCIII-PU-9333E0FB through 3.17.10 devices. There is a least privilege violation. **CVE ID : CVE-2020-11956**	N/A	O-RIT-CMCI-110820/1977
pdu-3c002dec_firmware					
Use of Hard-coded Credentials	7/14/2020	10	An issue was discovered on Rittal PDU-3C002DEC through 5.17.10 and CMCIII-PU-9333E0FB through 3.17.10 devices. There is a Backdoor root account. **CVE ID : CVE-2020-11951**	N/A	O-RIT-PDU--110820/1978
Information Exposure	7/14/2020	4.9	An issue was discovered on Rittal PDU-3C002DEC through 5.17.10 and CMCIII-PU-9333E0FB through 3.17.10 devices. Attackers can bypass the CLI menu. **CVE ID : CVE-2020-11952**	N/A	O-RIT-PDU--110820/1979
Improper Neutralization of Special	7/14/2020	9	An issue was discovered on Rittal PDU-3C002DEC through 5.15.40 and	N/A	O-RIT-PDU--110820/1980

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			CMCIII-PU-9333E0FB through 3.15.70_4 devices. Attackers can execute code. **CVE ID : CVE-2020-11953**		
Incorrect Default Permissions	7/14/2020	9	An issue was discovered on Rittal PDU-3C002DEC through 5.15.70 and CMCIII-PU-9333E0FB through 3.15.70 devices. There are insecure permissions. **CVE ID : CVE-2020-11955**	N/A	O-RIT-PDU--110820/1981
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	7/14/2020	10	An issue was discovered on Rittal PDU-3C002DEC through 5.17.10 and CMCIII-PU-9333E0FB through 3.17.10 devices. There is a least privilege violation. **CVE ID : CVE-2020-11956**	N/A	O-RIT-PDU--110820/1982
cmc_iii_pu_7030.000_firmware					
Use of Hard-coded Credentials	7/14/2020	10	An issue was discovered on Rittal PDU-3C002DEC through 5.17.10 and CMCIII-PU-9333E0FB through 3.17.10 devices. There is a Backdoor root account. **CVE ID : CVE-2020-11951**	N/A	O-RIT-CMC_-110820/1983
Information Exposure	7/14/2020	4.9	An issue was discovered on Rittal PDU-3C002DEC through 5.17.10 and CMCIII-PU-9333E0FB through 3.17.10 devices. Attackers can bypass the CLI menu. **CVE ID : CVE-2020-11952**	N/A	O-RIT-CMC_-110820/1984

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	7/14/2020	9	An issue was discovered on Rittal PDU-3C002DEC through 5.15.40 and CMCIII-PU-9333E0FB through 3.15.70_4 devices. Attackers can execute code. **CVE ID : CVE-2020-11953**	N/A	O-RIT-CMC_-110820/1985
Incorrect Default Permissions	7/14/2020	9	An issue was discovered on Rittal PDU-3C002DEC through 5.15.70 and CMCIII-PU-9333E0FB through 3.15.70 devices. There are insecure permissions. **CVE ID : CVE-2020-11955**	N/A	O-RIT-CMC_-110820/1986
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	7/14/2020	10	An issue was discovered on Rittal PDU-3C002DEC through 5.17.10 and CMCIII-PU-9333E0FB through 3.17.10 devices. There is a least privilege violation. **CVE ID : CVE-2020-11956**	N/A	O-RIT-CMC_-110820/1987
lcp-cw_firmware					
Use of Hard-coded Credentials	7/14/2020	10	An issue was discovered on Rittal PDU-3C002DEC through 5.17.10 and CMCIII-PU-9333E0FB through 3.17.10 devices. There is a Backdoor root account. **CVE ID : CVE-2020-11951**	N/A	O-RIT-LCP--110820/1988
Information Exposure	7/14/2020	4.9	An issue was discovered on Rittal PDU-3C002DEC through 5.17.10 and CMCIII-PU-9333E0FB through 3.17.10 devices.	N/A	O-RIT-LCP--110820/1989

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Attackers can bypass the CLI menu. **CVE ID : CVE-2020-11952**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	7/14/2020	9	An issue was discovered on Rittal PDU-3C002DEC through 5.15.40 and CMCIII-PU-9333E0FB through 3.15.70_4 devices. Attackers can execute code. **CVE ID : CVE-2020-11953**	N/A	O-RIT-LCP--110820/1990
Incorrect Default Permissions	7/14/2020	9	An issue was discovered on Rittal PDU-3C002DEC through 5.15.70 and CMCIII-PU-9333E0FB through 3.15.70 devices. There are insecure permissions. **CVE ID : CVE-2020-11955**	N/A	O-RIT-LCP--110820/1991
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	7/14/2020	10	An issue was discovered on Rittal PDU-3C002DEC through 5.17.10 and CMCIII-PU-9333E0FB through 3.17.10 devices. There is a least privilege violation. **CVE ID : CVE-2020-11956**	N/A	O-RIT-LCP--110820/1992
Siemens					
simatic_hmi_comfort_panels_firmware					
Cleartext Transmission of Sensitive Information	7/14/2020	3.3	A vulnerability has been identified in SIMATIC HMI Basic Panels 1st Generation (incl. SIPLUS variants) (All versions), SIMATIC HMI Basic Panels 2nd Generation (incl. SIPLUS variants) (All versions), SIMATIC HMI	N/A	O-SIE-SIMA-110820/1993

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Comfort Panels (incl. SIPLUS variants) (All versions), SIMATIC HMI KTP700F Mobile Arctic (All versions), SIMATIC HMI Mobile Panels 2nd Generation (All versions), SIMATIC WinCC Runtime Advanced (All versions). Unencrypted communication between the configuration software and the respective device could allow an attacker to capture potential plain text communication and have access to sensitive information. **CVE ID : CVE-2020-7592**		
sicam_mmu_firmware					
Out-of-bounds Read	7/14/2020	5	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). By performing a flooding attack against the web server, an attacker might be able to gain read access to the device's memory, possibly revealing confidential information. **CVE ID : CVE-2020-10037**	N/A	O-SIE-SICA-110820/1994
Missing Authentication for Critical Function	7/14/2020	7.5	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). An attacker with	N/A	O-SIE-SICA-110820/1995

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the device's web server might be able to execute administrative commands without authentication. **CVE ID : CVE-2020-10038**		
Missing Encryption of Sensitive Data	7/14/2020	6.8	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). An attacker in a privileged network position between a legitimate user and the web server might be able to conduct a Man-in-the-middle attack and gain read and write access to the transmitted data. **CVE ID : CVE-2020-10039**	N/A	O-SIE-SICA-110820/1996
Use of Password Hash With Insufficient Computational Effort	7/14/2020	2.1	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). An attacker with local access to the device might be able to retrieve some passwords in clear text. **CVE ID : CVE-2020-10040**	N/A	O-SIE-SICA-110820/1997
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/14/2020	4.3	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). A stored Cross-Site-Scripting (XSS)	N/A	O-SIE-SICA-110820/1998

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is present in different locations of the web application. An attacker might be able to take over a session of a legitimate user. **CVE ID : CVE-2020-10041**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/14/2020	7.5	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). A buffer overflow in various positions of the web application might enable an attacker with access to the web application to execute arbitrary code over the network. **CVE ID : CVE-2020-10042**	N/A	O-SIE-SICA-110820/1999
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/14/2020	4.3	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). The web server could allow Cross-Site Scripting (XSS) attacks if unsuspecting users are tricked into accessing a malicious link. **CVE ID : CVE-2020-10043**	N/A	O-SIE-SICA-110820/2000
Missing Authentication for Critical Function	7/14/2020	5	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). An attacker with	N/A	O-SIE-SICA-110820/2001

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the network could be able to install specially crafted firmware to the device. **CVE ID : CVE-2020-10044**		
Authentication Bypass by Capture-replay	7/14/2020	6.8	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). An error in the challenge-response procedure could allow an attacker to replay authentication traffic and gain access to protected areas of the web application. **CVE ID : CVE-2020-10045**	N/A	O-SIE-SICA-110820/2002
sicam_sgu_firmware					
Out-of-bounds Read	7/14/2020	5	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). By performing a flooding attack against the web server, an attacker might be able to gain read access to the device's memory, possibly revealing confidential information. **CVE ID : CVE-2020-10037**	N/A	O-SIE-SICA-110820/2003
Missing Authentication for Critical Function	7/14/2020	7.5	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions <	N/A	O-SIE-SICA-110820/2004

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V2.18). An attacker with access to the device's web server might be able to execute administrative commands without authentication. **CVE ID : CVE-2020-10038**		
Missing Encryption of Sensitive Data	7/14/2020	6.8	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). An attacker in a privileged network position between a legitimate user and the web server might be able to conduct a Man-in-the-middle attack and gain read and write access to the transmitted data. **CVE ID : CVE-2020-10039**	N/A	O-SIE-SICA-110820/2005
Use of Password Hash With Insufficient Computational Effort	7/14/2020	2.1	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). An attacker with local access to the device might be able to retrieve some passwords in clear text. **CVE ID : CVE-2020-10040**	N/A	O-SIE-SICA-110820/2006
Improper Neutralization of Input During Web Page Generation ('Cross-site	7/14/2020	4.3	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). A stored Cross-	N/A	O-SIE-SICA-110820/2007

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			Site-Scripting (XSS) vulnerability is present in different locations of the web application. An attacker might be able to take over a session of a legitimate user. **CVE ID : CVE-2020-10041**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/14/2020	7.5	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). A buffer overflow in various positions of the web application might enable an attacker with access to the web application to execute arbitrary code over the network. **CVE ID : CVE-2020-10042**	N/A	O-SIE-SICA-110820/2008
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/14/2020	4.3	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). The web server could allow Cross-Site Scripting (XSS) attacks if unsuspecting users are tricked into accessing a malicious link. **CVE ID : CVE-2020-10043**	N/A	O-SIE-SICA-110820/2009
Missing Authentication for Critical Function	7/14/2020	5	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions <	N/A	O-SIE-SICA-110820/2010

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V2.18). An attacker with access to the network could be able to install specially crafted firmware to the device. **CVE ID : CVE-2020-10044**		
Authentication Bypass by Capture-replay	7/14/2020	6.8	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). An error in the challenge-response procedure could allow an attacker to replay authentication traffic and gain access to protected areas of the web application. **CVE ID : CVE-2020-10045**	N/A	O-SIE-SICA-110820/2011
sicam_t_firmware					
Out-of-bounds Read	7/14/2020	5	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). By performing a flooding attack against the web server, an attacker might be able to gain read access to the device's memory, possibly revealing confidential information. **CVE ID : CVE-2020-10037**	N/A	O-SIE-SICA-110820/2012
Missing Authentication for Critical Function	7/14/2020	7.5	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions),	N/A	O-SIE-SICA-110820/2013

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SICAM T (All versions < V2.18). An attacker with access to the device's web server might be able to execute administrative commands without authentication. **CVE ID : CVE-2020-10038**		
Missing Encryption of Sensitive Data	7/14/2020	6.8	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). An attacker in a privileged network position between a legitimate user and the web server might be able to conduct a Man-in-the-middle attack and gain read and write access to the transmitted data. **CVE ID : CVE-2020-10039**	N/A	O-SIE-SICA-110820/2014
Use of Password Hash With Insufficient Computational Effort	7/14/2020	2.1	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). An attacker with local access to the device might be able to retrieve some passwords in clear text. **CVE ID : CVE-2020-10040**	N/A	O-SIE-SICA-110820/2015
Improper Neutralization of Input During Web Page Generation	7/14/2020	4.3	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions <	N/A	O-SIE-SICA-110820/2016

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			V2.18). A stored Cross-Site-Scripting (XSS) vulnerability is present in different locations of the web application. An attacker might be able to take over a session of a legitimate user. **CVE ID : CVE-2020-10041**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/14/2020	7.5	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). A buffer overflow in various positions of the web application might enable an attacker with access to the web application to execute arbitrary code over the network. **CVE ID : CVE-2020-10042**	N/A	O-SIE-SICA-110820/2017
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/14/2020	4.3	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). The web server could allow Cross-Site Scripting (XSS) attacks if unsuspecting users are tricked into accessing a malicious link. **CVE ID : CVE-2020-10043**	N/A	O-SIE-SICA-110820/2018
Missing Authentication for Critical Function	7/14/2020	5	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions),	N/A	O-SIE-SICA-110820/2019

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SICAM T (All versions < V2.18). An attacker with access to the network could be able to install specially crafted firmware to the device. **CVE ID : CVE-2020-10044**		
Authentication Bypass by Capture-replay	7/14/2020	6.8	A vulnerability has been identified in SICAM MMU (All versions < V2.05), SICAM SGU (All versions), SICAM T (All versions < V2.18). An error in the challenge-response procedure could allow an attacker to replay authentication traffic and gain access to protected areas of the web application. **CVE ID : CVE-2020-10045**	N/A	O-SIE-SICA-110820/2020
logo\!_8_bm_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/14/2020	7.5	A vulnerability has been identified in LOGO! 8 BM (incl. SIPLUS variants) (V1.81.01 - V1.81.03), LOGO! 8 BM (incl. SIPLUS variants) (V1.82.01), LOGO! 8 BM (incl. SIPLUS variants) (V1.82.02). A buffer overflow vulnerability exists in the Web Server functionality of the device. A remote unauthenticated attacker could send a specially crafted HTTP request to cause a memory corruption, potentially resulting in remote code	N/A	O-SIE-LOGO-110820/2021

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2020-7593**		
simatic_hmi_ktp700f_mobile_arctic_firmware					
Cleartext Transmission of Sensitive Information	7/14/2020	3.3	A vulnerability has been identified in SIMATIC HMI Basic Panels 1st Generation (incl. SIPLUS variants) (All versions), SIMATIC HMI Basic Panels 2nd Generation (incl. SIPLUS variants) (All versions), SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions), SIMATIC HMI KTP700F Mobile Arctic (All versions), SIMATIC HMI Mobile Panels 2nd Generation (All versions), SIMATIC WinCC Runtime Advanced (All versions). Unencrypted communication between the configuration software and the respective device could allow an attacker to capture potential plain text communication and have access to sensitive information. **CVE ID : CVE-2020-7592**	N/A	O-SIE-SIMA-110820/2022
simatic_hmi_mobile_panels_2nd_generation_firmware					
Cleartext Transmission of Sensitive Information	7/14/2020	3.3	A vulnerability has been identified in SIMATIC HMI Basic Panels 1st Generation (incl. SIPLUS variants) (All versions), SIMATIC HMI Basic Panels 2nd Generation (incl.	N/A	O-SIE-SIMA-110820/2023

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SIPLUS variants) (All versions), SIMATIC HMI Comfort Panels (incl. SIPLUS variants) (All versions), SIMATIC HMI KTP700F Mobile Arctic (All versions), SIMATIC HMI Mobile Panels 2nd Generation (All versions), SIMATIC WinCC Runtime Advanced (All versions). Unencrypted communication between the configuration software and the respective device could allow an attacker to capture potential plain text communication and have access to sensitive information. **CVE ID : CVE-2020-7592**		
simatic_s7-200_smart_sr_cpu_firmware					
Uncontrolled Resource Consumption	7/14/2020	5	A vulnerability has been identified in SIMATIC S7-200 SMART CPU family (All versions >= V2.2 < V2.5.1). Affected devices do not properly handle large numbers of new incomming connections and could crash under certain circumstances. An attacker may leverage this to cause a Denial-of-Service situation. **CVE ID : CVE-2020-7584**	N/A	O-SIE-SIMA-110820/2024
simatic_s7-200_smart_st_cpu_firmware					
Uncontrolled Resource	7/14/2020	5	A vulnerability has been identified in SIMATIC S7-	N/A	O-SIE-SIMA-110820/2025

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Consumption			200 SMART CPU family (All versions >= V2.2 < V2.5.1). Affected devices do not properly handle large numbers of new incomming connections and could crash under certain circumstances. An attacker may leverage this to cause a Denial-of-Service situation. **CVE ID : CVE-2020-7584**		
Sophos					
xg_firewall_firmware					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	7/10/2020	7.5	A SQL injection vulnerability in the user and admin web interfaces of Sophos XG Firewall v18.0 MR1 and older potentially allows an attacker to run arbitrary code remotely. The fix is built into the re-release of XG Firewall v18 MR-1 (named MR-1-Build396) and the v17.5 MR13 release. All other versions >= 17.0 have received a hotfix. **CVE ID : CVE-2020-15504**	https://community.sophos.com/b/security-blog/posts/advisory-resolved-rce-via-sqli-cve-2020-15504	O-SOP-XG_F-110820/2026
Tenda					
ac15_firmware					
Cross-Site Request Forgery (CSRF)	7/13/2020	7.1	A CSRF issue in the /goform/SysToolReboot endpoint of Tenda AC15 AC1900 version 15.03.05.19 allows remote attackers to reboot the device and cause denial of	N/A	O-TEN-AC15-110820/2027

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service via a payload hosted by an attacker-controlled web page. **CVE ID : CVE-2020-10986**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	7/13/2020	10	The goform/setUsbUnload endpoint of Tenda AC15 AC1900 version 15.03.05.19 allows remote attackers to execute arbitrary system commands via the deviceName POST parameter. **CVE ID : CVE-2020-10987**	N/A	O-TEN-AC15-110820/2028
Use of Hard-coded Credentials	7/13/2020	10	A hard-coded telnet credential in the tenda_login binary of Tenda AC15 AC1900 version 15.03.05.19 allows unauthenticated remote attackers to start a telnetd service on the device. **CVE ID : CVE-2020-10988**	N/A	O-TEN-AC15-110820/2029
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7/13/2020	4.3	An XSS issue in the /goform/WifiBasicSet endpoint of Tenda AC15 AC1900 version 15.03.05.19 allows remote attackers to execute malicious payloads via the WifiName POST parameter. **CVE ID : CVE-2020-10989**	N/A	O-TEN-AC15-110820/2030
ufactory					
xarm_5_lite_firmware					
Improper Restriction of Excessive	7/15/2020	7.5	The authentication implementation on the xArm controller has very	https://github.com/aliasrobotics/R	O-UFA-XARM-110820/2031

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication Attempts			low entropy, making it vulnerable to a brute-force attack. There is no mechanism in place to mitigate or lockout automated attempts to gain access. **CVE ID : CVE-2020-10285**	VD/issues/3322	
N/A	7/15/2020	5.8	the main user account has restricted privileges but is in the sudoers group and there is not any mechanism in place to prevent sudo su or sudo -i to be run gaining unrestricted access to sensible files, encryption, or issue orders that disrupt robot operation. **CVE ID : CVE-2020-10286**	https://github.com/aliasrobotics/RVD/issues/3323	O-UFA-XARM-110820/2032
xarm_6_firmware					
N/A	7/15/2020	5.8	the main user account has restricted privileges but is in the sudoers group and there is not any mechanism in place to prevent sudo su or sudo -i to be run gaining unrestricted access to sensible files, encryption, or issue orders that disrupt robot operation. **CVE ID : CVE-2020-10286**	https://github.com/aliasrobotics/RVD/issues/3323	O-UFA-XARM-110820/2033
xarm_7_firmware					
N/A	7/15/2020	5.8	the main user account has restricted privileges but is in the sudoers group and there is not any mechanism in place to	https://github.com/aliasrobotics/RVD/issues/	O-UFA-XARM-110820/2034

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prevent sudo su or sudo -i to be run gaining unrestricted access to sensible files, encryption, or issue orders that disrupt robot operation. **CVE ID : CVE-2020-10286**	3323	
ui					
unifi_protect_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	7/2/2020	6.5	We have recently released new version of UniFi Protect firmware v1.13.3 and v1.14.10 for Unifi Cloud Key Gen2 Plus and UniFi Dream Machine Pro/UNVR respectively that fixes vulnerabilities found on Protect firmware v1.13.2, v1.14.9 and prior according to the description below:View only users can run certain custom commands which allows them to assign themselves unauthorized roles and escalate their privileges. **CVE ID : CVE-2020-8188**	N/A	O-UI-UNIF-110820/2035
wavlink					
wl-wn530hg4_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	7/1/2020	10	An issue was discovered on Wavlink WL-WN530HG4 M30HG4.V5030.191116 devices. Multiple shell metacharacter injection vulnerabilities exist in CGI scripts, leading to remote code execution with root	N/A	O-WAV-WL-W-110820/2036

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges. **CVE ID : CVE-2020-15489**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	7/1/2020	10	An issue was discovered on Wavlink WL-WN530HG4 M30HG4.V5030.191116 devices. Multiple buffer overflow vulnerabilities exist in CGI scripts, leading to remote code execution with root privileges. (The set of affected scripts is similar to CVE-2020-12266.) **CVE ID : CVE-2020-15490**	N/A	O-WAV-WL-W-110820/2037
Windriver					
vxworks					
Improper Authentication	7/15/2020	7.5	IRC5 exposes an ftp server (port 21). Upon attempting to gain access you are challenged with a request of username and password, however you can input whatever you like. As long as the field isn't empty it will be accepted. **CVE ID : CVE-2020-10288**	https://github.com/aliasrobotics/RVD/issues/3327	O-WIN-VXWO-110820/2038
XEN					
xen					
Improper Input Validation	7/7/2020	4.7	An issue was discovered in Xen through 4.13.x, allowing x86 HVM guest OS users to cause a hypervisor crash. An inverted conditional in x86 HVM guests' dirty video RAM tracking code allows	N/A	O-XEN-XEN-110820/2039

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			such guests to make Xen de-reference a pointer guaranteed to point at unmapped space. A malicious or buggy HVM guest may cause the hypervisor to crash, resulting in Denial of Service (DoS) affecting the entire host. Xen versions from 4.8 onwards are affected. Xen versions 4.7 and earlier are not affected. Only x86 systems are affected. Arm systems are not affected. Only x86 HVM guests using shadow paging can leverage the vulnerability. In addition, there needs to be an entity actively monitoring a guest's video frame buffer (typically for display purposes) in order for such a guest to be able to leverage the vulnerability. x86 PV guests, as well as x86 HVM guests using hardware assisted paging (HAP), cannot leverage the vulnerability. **CVE ID : CVE-2020-15563**		
Improper Input Validation	7/7/2020	4.9	An issue was discovered in Xen through 4.13.x, allowing Arm guest OS users to cause a hypervisor crash because of a missing alignment check in VCPUOP_register_vcpu_info. The hypercall VCPUOP_register_vcpu_inf	N/A	O-XEN-XEN-110820/2040

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			o is used by a guest to register a shared region with the hypervisor. The region will be mapped into Xen address space so it can be directly accessed. On Arm, the region is accessed with instructions that require a specific alignment. Unfortunately, there is no check that the address provided by the guest will be correctly aligned. As a result, a malicious guest could cause a hypervisor crash by passing a misaligned address. A malicious guest administrator may cause a hypervisor crash, resulting in a Denial of Service (DoS). All Xen versions are vulnerable. Only Arm systems are vulnerable. x86 systems are not affected. **CVE ID : CVE-2020-15564**		
Uncontrolled Resource Consumption	7/7/2020	6.1	An issue was discovered in Xen through 4.13.x, allowing x86 Intel HVM guest OS users to cause a host OS denial of service or possibly gain privileges because of insufficient cache write-back under VT-d. When page tables are shared between IOMMU and CPU, changes to them require flushing of both TLBs. Furthermore, IOMMUs may be non-	N/A	O-XEN-XEN-110820/2041

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			coherent, and hence prior to flushing IOMMU TLBs, a CPU cache also needs writing back to memory after changes were made. Such writing back of cached data was missing in particular when splitting large page mappings into smaller granularity ones. A malicious guest may be able to retain read/write DMA access to frames returned to Xen's free pool, and later reused for another purpose. Host crashes (leading to a Denial of Service) and privilege escalation cannot be ruled out. Xen versions from at least 3.2 onwards are affected. Only x86 Intel systems are affected. x86 AMD as well as Arm systems are not affected. Only x86 HVM guests using hardware assisted paging (HAP), having a passed through PCI device assigned, and having page table sharing enabled can leverage the vulnerability. Note that page table sharing will be enabled (by default) only if Xen considers IOMMU and CPU large page size support compatible. **CVE ID : CVE-2020-15565**		
Improper Handling of	7/7/2020	4.7	An issue was discovered in Xen through 4.13.x,	N/A	O-XEN-XEN-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			allowing guest OS users to cause a host OS crash because of incorrect error handling in event-channel port allocation. The allocation of an event-channel port may fail for multiple reasons: (1) port is already in use, (2) the memory allocation failed, or (3) the port we try to allocate is higher than what is supported by the ABI (e.g., 2L or FIFO) used by the guest or the limit set by an administrator (max_event_channels in xl cfg). Due to the missing error checks, only (1) will be considered an error. All the other cases will provide a valid port and will result in a crash when trying to access the event channel. When the administrator configured a guest to allow more than 1023 event channels, that guest may be able to crash the host. When Xen is out-of-memory, allocation of new event channels will result in crashing the host rather than reporting an error. Xen versions 4.10 and later are affected. All architectures are affected. The default configuration, when guests are created with xl/libxl, is not vulnerable, because of the		110820/2042

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			default event-channel limit. **CVE ID : CVE-2020-15566**		
Improper Privilege Management	7/7/2020	4.4	An issue was discovered in Xen through 4.13.x, allowing Intel guest OS users to gain privileges or cause a denial of service because of non-atomic modification of a live EPT PTE. When mapping guest EPT (nested paging) tables, Xen would in some circumstances use a series of non-atomic bitfield writes. Depending on the compiler version and optimisation flags, Xen might expose a dangerous partially written PTE to the hardware, which an attacker might be able to race to exploit. A guest administrator or perhaps even an unprivileged guest user might be able to cause denial of service, data corruption, or privilege escalation. Only systems using Intel CPUs are vulnerable. Systems using AMD CPUs, and Arm systems, are not vulnerable. Only systems using nested paging (hap, aka nested paging, aka in this case Intel EPT) are vulnerable. Only HVM and PVH guests can exploit the vulnerability. The presence and scope of the	N/A	O-XEN-XEN-110820/2043

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability depends on the precise optimisations performed by the compiler used to build Xen. If the compiler generates (a) a single 64-bit write, or (b) a series of read-modify-write operations in the same order as the source code, the hypervisor is not vulnerable. For example, in one test build using GCC 8.3 with normal settings, the compiler generated multiple (unlocked) read-modify-write operations in source-code order, which did not constitute a vulnerability. We have not been able to survey compilers; consequently we cannot say which compiler(s) might produce vulnerable code (with which code-generation options). The source code clearly violates the C rules, and thus should be considered vulnerable. **CVE ID : CVE-2020-15567**		
yubico					
yubikey_5_nfc_firmware					
N/A	7/9/2020	4.3	A PIN management problem was discovered on Yubico YubiKey 5 devices 5.2.0 to 5.2.6. OpenPGP has three passwords: Admin PIN, Reset Code, and User PIN. The Reset Code is used to	https://www.yubico.com/support/security-advisories/ysa-2020-05/	O-YUB-YUBI-110820/2044

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reset the User PIN, but it is disabled by default. A flaw in the implementation of OpenPGP sets the Reset Code to a known value upon initialization. If the retry counter for the Reset Code is set to non-zero without changing the Reset Code, this known value can be used to reset the User PIN. To set the retry counters, the Admin PIN is required. **CVE ID : CVE-2020-15000**		
Information Exposure	7/9/2020	2.9	An information leak was discovered on Yubico YubiKey 5 NFC devices 5.0.0 to 5.2.6 and 5.3.0 to 5.3.1. The OTP application allows a user to set optional access codes on OTP slots. This access code is intended to prevent unauthorized changes to OTP configurations. The access code is not checked when updating NFC specific components of the OTP configurations. This may allow an attacker to access configured OTPs and passwords stored in slots that were not configured by the user to be read over NFC, despite a user having set an access code. (Users who have not set an access code, or who have not configured the OTP slots, are not	https://www.yubico.com/support/security-advisories/ysa-2020-04/	O-YUB-YUBI-110820/2045

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			impacted by this issue.) **CVE ID : CVE-2020-15001**		