National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures(CVE) Report

16 - 31 Oct 2020 Vol. 07 No. 20

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
1password					
command-line					
Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG)	27-Oct-20	5	An issue was discovered in beta versions of the 1Password command-line tool prior to 0.5.5 and in beta versions of the 1Password SCIM bridge prior to 0.7.3. An insecure random number generator was used to generate various keys. An attacker with access to the user's encrypted data may be able to perform brute-force calculations of encryption keys and thus succeed at decryption. **CVE ID : CVE-2020-10256**	https://support.1password.com/kb/202010/	A-1PA-COMM-031120/1
scim					
Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG)	27-Oct-20	5	An issue was discovered in beta versions of the 1Password command-line tool prior to 0.5.5 and in beta versions of the 1Password SCIM bridge prior to 0.7.3. An insecure random number generator was used to generate various keys. An attacker with access to the user's encrypted data may be able to perform brute-force calculations of encryption keys and thus succeed at	https://support.1password.com/kb/202010/	A-1PA-SCIM-031120/2

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			decryption. **CVE ID : CVE-2020-10256**		
Acronis					
cyber_protect					
Improper Privilege Management	21-Oct-20	7.2	Acronis Cyber Backup 12.5 and Cyber Protect 15 include an OpenSSL component that specifies an OPENSSLDIR variable as a subdirectory within C:\jenkins_agent\. Acronis Cyber Backup and Cyber Protect contain a privileged service that uses this OpenSSL component. Because unprivileged Windows users can create subdirectories off of the system root, a user can create the appropriate path to a specially-crafted openssl.cnf file to achieve arbitrary code execution with SYSTEM privileges. **CVE ID : CVE-2020-10138**	N/A	A-ACR-CYBE-031120/3
true_image					
Improper Privilege Management	21-Oct-20	7.2	Acronis True Image 2021 includes an OpenSSL component that specifies an OPENSSLDIR variable as a subdirectory within C:\jenkins_agent\. Acronis True Image contains a privileged service that uses this OpenSSL component. Because unprivileged Windows users can create subdirectories off of the system root, a user can create the appropriate path to a	N/A	A-ACR-TRUE-031120/4

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specially-crafted openssl.cnf file to achieve arbitrary code execution with SYSTEM privileges. **CVE ID : CVE-2020-10139**		
Incorrect Permission Assignment for Critical Resource	21-Oct-20	6.9	Acronis True Image 2021 fails to properly set ACLs of the C:\ProgramData\Acronis directory. Because some privileged processes are executed from the C:\ProgramData\Acronis, an unprivileged user can achieve arbitrary code execution with SYSTEM privileges by placing a DLL in one of several paths within C:\ProgramData\Acronis. **CVE ID : CVE-2020-10140**	N/A	A-ACR-TRUE-031120/5
cyber_backup					
Improper Privilege Management	21-Oct-20	7.2	Acronis Cyber Backup 12.5 and Cyber Protect 15 include an OpenSSL component that specifies an OPENSSLDIR variable as a subdirectory within C:\jenkins_agent\. Acronis Cyber Backup and Cyber Protect contain a privileged service that uses this OpenSSL component. Because unprivileged Windows users can create subdirectories off of the system root, a user can create the appropriate path to a specially-crafted openssl.cnf file to achieve arbitrary code execution with SYSTEM privileges.	N/A	A-ACR-CYBE-031120/6

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-10138		
Adobe					
after_effects					
Out-of-bounds Read	21-Oct-20	9.3	Adobe After Effects version 17.1.1 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted .aepx file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. This vulnerability requires user interaction to exploit. **CVE ID : CVE-2020-24418**	N/A	A-ADO-AFTE-031120/7
Uncontrolled Search Path Element	21-Oct-20	6.9	Adobe After Effects version 17.1.1 (and earlier) for Windows is affected by an uncontrolled search path vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2020-24419**	N/A	A-ADO-AFTE-031120/8
photoshop					
Uncontrolled Search Path Element	21-Oct-20	6.9	Adobe Photoshop for Windows version 21.2.1 (and earlier) is affected by an uncontrolled search path element vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation	N/A	A-ADO-PHOT-031120/9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2020-24420**		
media_encoder					
Uncontrolled Search Path Element	21-Oct-20	6.9	Adobe Media Encoder version 14.4 (and earlier) for Windows is affected by an uncontrolled search path vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2020-24423**	N/A	A-ADO-MEDI-031120/10
marketo_sales_insight					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-20	4.3	Marketo Sales Insight plugin version 1.4355 (and earlier) is affected by a blind stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2020-24416**	N/A	A-ADO-MARK-031120/11
animate					
Double Free	21-Oct-20	9.3	Adobe Animate version 20.5 (and earlier) is affected by a double free vulnerability when parsing a crafted .fla file, which could result in	N/A	A-ADO-ANIM-031120/12

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution in the context of the current user. This vulnerability requires user interaction to exploit. **CVE ID : CVE-2020-9747**		
Out-of-bounds Read	21-Oct-20	9.3	Adobe Animate version 20.5 (and earlier) is affected by an out-of-bounds read vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted .fla file in Animate. **CVE ID : CVE-2020-9749**	N/A	A-ADO-ANIM-031120/13
Out-of-bounds Read	21-Oct-20	9.3	Adobe Animate version 20.5 (and earlier) is affected by an out-of-bounds read vulnerability, which could result in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted .fla file in Animate. **CVE ID : CVE-2020-9750**	N/A	A-ADO-ANIM-031120/14
illustrator					
Out-of-bounds Read	20-Oct-20	6.8	Adobe Illustrator version 24.2 (and earlier) is affected by an out-of-bounds read vulnerability when parsing crafted PDF files. This could result in a read past the end of an allocated memory structure, potentially resulting in arbitrary code execution in the context of	N/A	A-ADO-ILLU-031120/15

CVSS Scoring Scale	0-1	1-2	2-3	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 current user. This vulnerability requires user interaction to exploit. **CVE ID : CVE-2020-24409**		
Out-of-bounds Read	20-Oct-20	6.8	Adobe Illustrator version 24.2 (and earlier) is affected by an out-of-bounds read vulnerability when parsing crafted PDF files. This could result in a read past the end of an allocated memory structure, potentially resulting in arbitrary code execution in the context of the current user. This vulnerability requires user interaction to exploit. **CVE ID : CVE-2020-24410**	N/A	A-ADO-ILLU-031120/16
Out-of-bounds Write	20-Oct-20	6.8	Adobe Illustrator version 24.2 (and earlier) is affected by an out-of-bounds write vulnerability when handling crafted PDF files. This could result in a write past the end of an allocated memory structure, potentially resulting in arbitrary code execution in the context of the current user. This vulnerability requires user interaction to exploit. **CVE ID : CVE-2020-24411**	N/A	A-ADO-ILLU-031120/17
Improper Restriction of Operations within the Bounds of a Memory	20-Oct-20	6.8	Adobe Illustrator version 24.1.2 (and earlier) is affected by a memory corruption vulnerability that occurs when parsing a specially crafted .svg file. This could result in arbitrary code	N/A	A-ADO-ILLU-031120/18

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			execution in the context of the current user. This vulnerability requires user interaction to exploit. **CVE ID : CVE-2020-24412**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-20	6.8	Adobe Illustrator version 24.1.2 (and earlier) is affected by a memory corruption vulnerability that occurs when parsing a specially crafted .svg file. This could result in arbitrary code execution in the context of the current user. This vulnerability requires user interaction to exploit. **CVE ID : CVE-2020-24413**	N/A	A-ADO-ILLU-031120/19
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-20	6.8	Adobe Illustrator version 24.1.2 (and earlier) is affected by a memory corruption vulnerability that occurs when parsing a specially crafted .svg file. This could result in arbitrary code execution in the context of the current user. This vulnerability requires user interaction to exploit. **CVE ID : CVE-2020-24414**	N/A	A-ADO-ILLU-031120/20
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-20	6.8	Adobe Illustrator version 24.1.2 (and earlier) is affected by a memory corruption vulnerability that occurs when parsing a specially crafted .svg file. This could result in arbitrary code execution in the context of the current user. This vulnerability requires user	N/A	A-ADO-ILLU-031120/21

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction to exploit. **CVE ID : CVE-2020-24415**		
Advantech					
r-seenet					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Oct-20	5	The R-SeeNet webpage (1.5.1 through 2.4.10) suffers from SQL injection, which allows a remote attacker to invoke queries on the database and retrieve sensitive information. **CVE ID : CVE-2020-25157**	N/A	A-ADV-R-SE-031120/22
Amazon					
firecracker					
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Oct-20	5	In Amazon AWS Firecracker before 0.21.3, and 0.22.x before 0.22.1, the serial console buffer can grow its memory usage without limit when data is sent to the standard input. This can result in a memory leak on the microVM emulation thread, possibly occupying more memory than intended on the host. **CVE ID : CVE-2020-27174**	N/A	A-AMA-FIRE-031120/23
antsword_project					
antsword					
Improper Neutralization of Input During Web Page Generation ('Cross-site	26-Oct-20	6.8	A cross-site scripting (XSS) vulnerability AntSword v2.0.7 can remotely execute system commands. **CVE ID : CVE-2020-18766**	N/A	A-ANT-ANTS-031120/24

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-20	4.3	AntSword 2.1.8.1 contains a cross-site scripting (XSS) vulnerability in the View Site funtion. When viewing an added site, an XSS payload can be injected in cookies view which can lead to remote code execution. **CVE ID : CVE-2020-25470**	N/A	A-ANT-ANTS-031120/25
anuko					
time_tracker					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	16-Oct-20	6.5	In Anuko Time Tracker before verion 1.19.23.5325, due to not properly filtered user input a CSV export of a report could contain cells that are treated as formulas by spreadsheet software (for example, when a cell value starts with an equal sign). This is fixed in version 1.19.23.5325. **CVE ID : CVE-2020-15255**	https://github.com/anuko/timetracker/security/advisories/GHSA-prjf-9mgh-8fpv	A-ANU-TIME-031120/26
Apache					
kylin					
Insecure Storage of Sensitive Information	19-Oct-20	5	Apache Kylin 2.0.0, 2.1.0, 2.2.0, 2.3.0, 2.3.1, 2.3.2, 2.4.0, 2.4.1, 2.5.0, 2.5.1, 2.5.2, 2.6.0, 2.6.1, 2.6.2, 2.6.3, 2.6.4, 2.6.5, 2.6.6, 3.0.0-alpha, 3.0.0-alpha2, 3.0.0-beta, 3.0.0, 3.0.1, 3.0.2, 3.1.0, 4.0.0-alpha has one restful api which exposed Kylin's configuration information without any authentication, so it is dangerous because some	N/A	A-APA-KYLI-031120/27

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			confidential information entries will be disclosed to everyone. **CVE ID : CVE-2020-13937**		
Apereo					
central_authentication_service					
Improper Authentication	16-Oct-20	5	Apereo CAS 5.3.x before 5.3.16, 6.x before 6.1.7.2, 6.2.x before 6.2.4, and 6.3.x before 6.3.0-RC4 mishandles secret keys with Google Authenticator for multifactor authentication. **CVE ID : CVE-2020-27178**	N/A	A-APE-CENT-031120/28
Apple					
xcode					
N/A	16-Oct-20	9.3	This issue was addressed by encrypting communications over the network to devices running iOS 14, iPadOS 14, tvOS 14, and watchOS 7. This issue is fixed in iOS 14.0 and iPadOS 14.0, Xcode 12.0. An attacker in a privileged network position may be able to execute arbitrary code on a paired device during a debug session over the network. **CVE ID : CVE-2020-9992**	N/A	A-APP-XCOD-031120/29
icloud					
Origin Validation Error	27-Oct-20	7.2	A logic issue was addressed with improved validation. This issue is fixed in iCloud for Windows 7.17, iTunes 12.10.4 for Windows, iCloud for Windows 10.9.2, tvOS 13.3.1, Safari 13.0.5, iOS 13.3.1 and iPadOS 13.3.1. A	N/A	A-APP-ICLO-031120/30

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			DOM object context may not have had a unique security origin. **CVE ID : CVE-2020-3864**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Oct-20	6.8	A command injection issue existed in Web Inspector. This issue was addressed with improved escaping. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Copying a URL from Web Inspector may lead to command injection. **CVE ID : CVE-2020-9862**	N/A	A-APP-ICLO-031120/31
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9871**	N/A	A-APP-ICLO-031120/32
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8	N/A	A-APP-ICLO-031120/33

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9872**		
Out-of-bounds Read	22-Oct-20	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9873**	N/A	A-APP-ICLO-031120/34
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9874**	N/A	A-APP-ICLO-031120/35
Integer Overflow or Wraparound	22-Oct-20	6.8	An integer overflow was addressed through improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6,	N/A	A-APP-ICLO-031120/36

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9875**		
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Opening a maliciously crafted PDF file may lead to an unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9876**	N/A	A-APP-ICLO-031120/37
Out-of-bounds Read	22-Oct-20	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9877**	N/A	A-APP-ICLO-031120/38
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking.	N/A	A-APP-ICLO-031120/39

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
			This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9879**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Oct-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9883**	N/A	A-APP-ICLO-031120/40
Use After Free	16-Oct-20	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9893**	N/A	A-APP-ICLO-031120/41

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Oct-20	4.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9894**	N/A	A-APP-ICLO-031120/42
Use After Free	16-Oct-20	7.5	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9895**	N/A	A-APP-ICLO-031120/43
Improper Authenticati on	16-Oct-20	6.5	Multiple issues were addressed with improved logic. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A malicious attacker with arbitrary read and write capability may be able to bypass Pointer	N/A	A-APP-ICLO-031120/44

CVSS Scoring Scale	0-1	1-2	2-3	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. **CVE ID : CVE-2020-9910**		
N/A	16-Oct-20	4.3	An access issue existed in Content Security Policy. This issue was addressed with improved access restrictions. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing maliciously crafted web content may prevent Content Security Policy from being enforced. **CVE ID : CVE-2020-9915**	N/A	A-APP-ICLO-031120/45
N/A	16-Oct-20	5	A URL Unicode encoding issue was addressed with improved state management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A malicious attacker may be able to conceal the destination of a URL. **CVE ID : CVE-2020-9916**	N/A	A-APP-ICLO-031120/46
Out-of-bounds Write	22-Oct-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for	N/A	A-APP-ICLO-031120/47

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9919**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-20	4.3	A logic issue was addressed with improved state management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2020-9925**	N/A	A-APP-ICLO-031120/48
Out-of-bounds Write	16-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9936**	N/A	A-APP-ICLO-031120/49
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8	N/A	A-APP-ICLO-031120/50

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
			for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9937**		
Out-of-bounds Read	22-Oct-20	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9938**	N/A	A-APP-ICLO-031120/51
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-20	4.3	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 14.0 and iPadOS 14.0, tvOS 14.0, watchOS 7.0, Safari 14.0, iCloud for Windows 11.4, iCloud for Windows 7.21. Processing maliciously crafted web content may lead to a cross site scripting attack. **CVE ID : CVE-2020-9952**	N/A	A-APP-ICLO-031120/52
Out-of-bounds Read	22-Oct-20	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows,	N/A	A-APP-ICLO-031120/53

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9984**		
itunes					
Origin Validation Error	27-Oct-20	7.2	A logic issue was addressed with improved validation. This issue is fixed in iCloud for Windows 7.17, iTunes 12.10.4 for Windows, iCloud for Windows 10.9.2, tvOS 13.3.1, Safari 13.0.5, iOS 13.3.1 and iPadOS 13.3.1. A DOM object context may not have had a unique security origin. **CVE ID : CVE-2020-3864**	N/A	A-APP-ITUN-031120/54
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Oct-20	6.8	A command injection issue existed in Web Inspector. This issue was addressed with improved escaping. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Copying a URL from Web Inspector may lead to command injection. **CVE ID : CVE-2020-9862**	N/A	A-APP-ITUN-031120/55
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8,	N/A	A-APP-ITUN-031120/56

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9871**		
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9872**	N/A	A-APP-ITUN-031120/57
Out-of-bounds Read	22-Oct-20	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9873**	N/A	A-APP-ITUN-031120/58
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6	N/A	A-APP-ITUN-031120/59

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9874**		
Integer Overflow or Wraparound	22-Oct-20	6.8	An integer overflow was addressed through improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9875**	N/A	A-APP-ITUN-031120/60
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Opening a maliciously crafted PDF file may lead to an unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9876**	N/A	A-APP-ITUN-031120/61
Out-of-	22-Oct-20	6.8	An out-of-bounds read was	N/A	A-APP-ITUN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9877**		031120/62
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9879**	N/A	A-APP-ITUN-031120/63
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Oct-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution.	N/A	A-APP-ITUN-031120/64

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9883		
Use After Free	16-Oct-20	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9893**	N/A	A-APP-ITUN-031120/65
Out-of-bounds Read	16-Oct-20	4.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9894**	N/A	A-APP-ITUN-031120/66
Use After Free	16-Oct-20	7.5	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A remote attacker may be able to cause unexpected	N/A	A-APP-ITUN-031120/67

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
			application termination or arbitrary code execution. **CVE ID : CVE-2020-9895**		
Improper Authentication	16-Oct-20	6.5	Multiple issues were addressed with improved logic. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A malicious attacker with arbitrary read and write capability may be able to bypass Pointer Authentication. **CVE ID : CVE-2020-9910**	N/A	A-APP-ITUN-031120/68
N/A	16-Oct-20	4.3	An access issue existed in Content Security Policy. This issue was addressed with improved access restrictions. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing maliciously crafted web content may prevent Content Security Policy from being enforced. **CVE ID : CVE-2020-9915**	N/A	A-APP-ITUN-031120/69
N/A	16-Oct-20	5	A URL Unicode encoding issue was addressed with improved state management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows,	N/A	A-APP-ITUN-031120/70

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			iCloud for Windows 11.3, iCloud for Windows 7.20. A malicious attacker may be able to conceal the destination of a URL. **CVE ID : CVE-2020-9916**		
Out-of-bounds Write	22-Oct-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9919**	N/A	A-APP-ITUN-031120/71
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-20	4.3	A logic issue was addressed with improved state management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2020-9925**	N/A	A-APP-ITUN-031120/72
Out-of-bounds Write	16-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8,	N/A	A-APP-ITUN-031120/73

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9936**		
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9937**	N/A	A-APP-ITUN-031120/74
Out-of-bounds Read	22-Oct-20	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9938**	N/A	A-APP-ITUN-031120/75
Out-of-bounds Read	22-Oct-20	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS	N/A	A-APP-ITUN-031120/76

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9984**		
safari					
Origin Validation Error	27-Oct-20	7.2	A logic issue was addressed with improved validation. This issue is fixed in iCloud for Windows 7.17, iTunes 12.10.4 for Windows, iCloud for Windows 10.9.2, tvOS 13.3.1, Safari 13.0.5, iOS 13.3.1 and iPadOS 13.3.1. A DOM object context may not have had a unique security origin. **CVE ID : CVE-2020-3864**	N/A	A-APP-SAFA-031120/77
N/A	27-Oct-20	5.8	A custom URL scheme handling issue was addressed with improved input validation. This issue is fixed in Safari 13.0.5. Processing a maliciously crafted URL may lead to arbitrary javascript code execution. **CVE ID : CVE-2020-9860**	N/A	A-APP-SAFA-031120/78
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Oct-20	6.8	A command injection issue existed in Web Inspector. This issue was addressed with improved escaping. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows,	N/A	A-APP-SAFA-031120/79

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			iCloud for Windows 11.3, iCloud for Windows 7.20. Copying a URL from Web Inspector may lead to command injection. **CVE ID : CVE-2020-9862**		
Use After Free	16-Oct-20	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9893**	N/A	A-APP-SAFA-031120/80
Out-of-bounds Read	16-Oct-20	4.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9894**	N/A	A-APP-SAFA-031120/81
Use After Free	16-Oct-20	7.5	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8,	N/A	A-APP-SAFA-031120/82

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9895**		
Origin Validation Error	16-Oct-20	5	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.6 and iPadOS 13.6, Safari 13.1.2. A malicious attacker may cause Safari to suggest a password for the wrong domain. **CVE ID : CVE-2020-9903**	N/A	A-APP-SAFA-031120/83
Improper Authenticati on	16-Oct-20	6.5	Multiple issues were addressed with improved logic. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A malicious attacker with arbitrary read and write capability may be able to bypass Pointer Authentication. **CVE ID : CVE-2020-9910**	N/A	A-APP-SAFA-031120/84
N/A	16-Oct-20	5	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.6 and iPadOS 13.6, Safari 13.1.2. An issue in Safari Reader mode may allow a remote attacker to bypass the	N/A	A-APP-SAFA-031120/85

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Same Origin Policy. **CVE ID : CVE-2020-9911**		
N/A	16-Oct-20	2.1	A logic issue was addressed with improved restrictions. This issue is fixed in Safari 13.1.2. A malicious attacker may be able to change the origin of a frame for a download in Safari Reader mode. **CVE ID : CVE-2020-9912**	N/A	A-APP-SAFA-031120/86
N/A	16-Oct-20	4.3	An access issue existed in Content Security Policy. This issue was addressed with improved access restrictions. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing maliciously crafted web content may prevent Content Security Policy from being enforced. **CVE ID : CVE-2020-9915**	N/A	A-APP-SAFA-031120/87
N/A	16-Oct-20	5	A URL Unicode encoding issue was addressed with improved state management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A malicious attacker may be able to conceal the destination of a URL. **CVE ID : CVE-2020-9916**	N/A	A-APP-SAFA-031120/88

CVSS Scoring Scale	0-1	1-2	2-3	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')	16-Oct-20	4.3	A logic issue was addressed with improved state management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2020-9925**	N/A	A-APP-SAFA-031120/89
Out-of-bounds Write	16-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9936**	N/A	A-APP-SAFA-031120/90
Access of Resource Using Incompatible Type ('Type Confusion')	16-Oct-20	6.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in Safari 14.0. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9948**	N/A	A-APP-SAFA-031120/91
Use After Free	16-Oct-20	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in Safari 14.0.	N/A	A-APP-SAFA-031120/92

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-9951**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-20	4.3	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 14.0 and iPadOS 14.0, tvOS 14.0, watchOS 7.0, Safari 14.0, iCloud for Windows 11.4, iCloud for Windows 7.21. Processing maliciously crafted web content may lead to a cross site scripting attack. **CVE ID : CVE-2020-9952**	N/A	A-APP-SAFA-031120/93
Out-of-bounds Write	16-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in Safari 14.0. Processing maliciously crafted web content may lead to code execution. **CVE ID : CVE-2020-9983**	N/A	A-APP-SAFA-031120/94
music					
Missing Authorization	27-Oct-20	4.3	This issue was addressed with improved checks to prevent unauthorized actions. This issue is fixed in Apple Music 3.4.0 for Android. A malicious application may be able to leak a user's credentials. **CVE ID : CVE-2020-9982**	N/A	A-APP-MUSI-031120/95
Appneta					
tcpreplay					
Out-of-bounds	19-Oct-20	5	An issue was discovered in tcpreplay tcpprep v4.3.3.	N/A	A-APP-TCPR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			There is a heap buffer overflow vulnerability in MemcmpInterceptorCommon () that can make tcpprep crash and cause a denial of service. **CVE ID : CVE-2020-24265**		031120/96
Out-of-bounds Write	19-Oct-20	5	An issue was discovered in tcpreplay tcpprep v4.3.3. There is a heap buffer overflow vulnerability in get_l2len() that can make tcpprep crash and cause a denial of service. **CVE ID : CVE-2020-24266**	N/A	A-APP-TCPR-031120/97
aptean					
product_configurator					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Oct-20	7.5	An issue was discovered in Aptean Product Configurator 4.61.0000 on Windows. A Time based SQL injection affects the nameTxt parameter on the main login page (aka cse?cmd=LOGIN). This can be exploited directly, and remotely. **CVE ID : CVE-2020-26944**	N/A	A-APT-PROD-031120/98
Arubanetworks					
airwave_glass					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	26-Oct-20	9	A remote execution of arbitrary commands vulnerability was discovered in Aruba Airwave Software version(s): Prior to 1.3.2. **CVE ID : CVE-2020-24631**	N/A	A-ARU-AIRW-031120/99

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	26-Oct-20	9	A remote execution of arbitrary commandss vulnerability was discovered in Aruba Airwave Software version(s): Prior to 1.3.2. **CVE ID : CVE-2020-24632**	N/A	A-ARU-AIRW-031120/100
Missing Authorization	26-Oct-20	7.5	A remote unauthorized access vulnerability was discovered in Aruba Airwave Software version(s): Prior to 1.3.2. **CVE ID : CVE-2020-7124**	N/A	A-ARU-AIRW-031120/101
Improper Privilege Management	26-Oct-20	6.5	A remote escalation of privilege vulnerability was discovered in Aruba Airwave Software version(s): Prior to 1.3.2. **CVE ID : CVE-2020-7125**	N/A	A-ARU-AIRW-031120/102
Server-Side Request Forgery (SSRF)	26-Oct-20	5	A remote server-side request forgery (ssrf) vulnerability was discovered in Aruba Airwave Software version(s): Prior to 1.3.2. **CVE ID : CVE-2020-7126**	N/A	A-ARU-AIRW-031120/103
N/A	26-Oct-20	7.5	A remote unauthenticated arbitrary code execution vulnerability was discovered in Aruba Airwave Software version(s): Prior to 1.3.2. **CVE ID : CVE-2020-7127**	N/A	A-ARU-AIRW-031120/104
atomx					
atomxcms					
Missing Authorization	22-Oct-20	5.5	AtomXCMS 2.0 is affected by Incorrect Access Control via admin/dump.php	N/A	A-ATO-ATOM-031120/105

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-26649		
Missing Authorization	22-Oct-20	5	AtomXCMS 2.0 is affected by Arbitrary File Read via admin/dump.php **CVE ID : CVE-2020-26650**	N/A	A-ATO-ATOM-031120/106
auth0					
omniauth-auth0					
Improper Verification of Cryptographic Signature	21-Oct-20	5.8	omniauth-auth0 (rubygems) versions >= 2.3.0 and < 2.4.1 improperly validate the JWT token signature when using the `jwt_validator.verify` method. Improper validation of the JWT token signature can allow an attacker to bypass authentication and authorization. You are affected by this vulnerability if all of the following conditions apply: 1. You are using `omniauth-auth0`. 2. You are using `JWTValidator.verify` method directly OR you are not authenticating using the SDK's default Authorization Code Flow. The issue is patched in version 2.4.1. **CVE ID : CVE-2020-15240**	https://github.com/auth0/omniauth-auth0/security/advisories/GHSA-58r4-h6v8-jcvm	A-AUT-OMNI-031120/107
bigbluebutton					
bigbluebutton					
Server-Side Request Forgery (SSRF)	21-Oct-20	4	BigBlueButton before 2.2.7 allows remote authenticated users to read local files and conduct SSRF attacks via an uploaded Office document that has a crafted URL in an ODF xlink field.	N/A	A-BIG-BIGB-031120/108

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-25820		
N/A	21-Oct-20	5	BigBlueButton before 2.2.27 has an unsafe JODConverter setting in which LibreOffice document conversions can access external files. **CVE ID : CVE-2020-27603**	N/A	A-BIG-BIGB-031120/109
Improper Encoding or Escaping of Output	21-Oct-20	4	BigBlueButton before 2.3 does not implement LibreOffice sandboxing. This might make it easier for remote authenticated users to read the API shared secret in the bigbluebutton.properties file. With the API shared secret, an attacker can (for example) use api/join to join an arbitrary meeting regardless of its guestPolicy setting. **CVE ID : CVE-2020-27604**	N/A	A-BIG-BIGB-031120/110
N/A	21-Oct-20	7.5	BigBlueButton through 2.2.28 uses Ghostscript for processing of uploaded EPS documents, and consequently may be subject to attacks related to a "schwache Sandbox." **CVE ID : CVE-2020-27605**	N/A	A-BIG-BIGB-031120/111
N/A	21-Oct-20	5	BigBlueButton before 2.2.28 (or earlier) does not set the secure flag for the session cookie in an https session, which makes it easier for remote attackers to capture this cookie by intercepting its transmission within an http session.	N/A	A-BIG-BIGB-031120/112

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-27606		
N/A	21-Oct-20	6.4	In BigBlueButton before 2.2.28 (or earlier), the client-side Mute button only signifies that the server should stop accepting audio data from the client. It does not directly configure the client to stop sending audio data to the server, and thus a modified server could store the audio data and/or transmit it to one or more meeting participants or other third parties. **CVE ID : CVE-2020-27607**	N/A	A-BIG-BIGB-031120/113
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Oct-20	4.3	In BigBlueButton before 2.2.28 (or earlier), uploaded presentations are sent to clients without a Content-Type header, which allows XSS, as demonstrated by a .png file extension for an HTML document. **CVE ID : CVE-2020-27608**	N/A	A-BIG-BIGB-031120/114
Incorrect Authorization	21-Oct-20	5	BigBlueButton through 2.2.28 records a video meeting despite the deactivation of video recording in the user interface. This may result in data storage beyond what is authorized for a specific meeting topic or participant. **CVE ID : CVE-2020-27609**	N/A	A-BIG-BIGB-031120/115
Information Exposure	21-Oct-20	5	The installation procedure in BigBlueButton before 2.2.28 (or earlier) exposes certain network services to external interfaces, and does not	N/A	A-BIG-BIGB-031120/116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			automatically set up a firewall configuration to block external access. **CVE ID : CVE-2020-27610**		
Use of a Broken or Risky Cryptographic Algorithm	21-Oct-20	7.5	BigBlueButton through 2.2.28 uses STUN/TURN resources from a third party, which may represent an unintended endpoint. **CVE ID : CVE-2020-27611**	N/A	A-BIG-BIGB-031120/117
Information Exposure	21-Oct-20	4	Greenlight in BigBlueButton through 2.2.28 places usernames in room URLs, which may represent an unintended information leak to users in a room, or an information leak to outsiders if any user publishes a screenshot of a browser window. **CVE ID : CVE-2020-27612**	N/A	A-BIG-BIGB-031120/118
Cleartext Storage of Sensitive Information	21-Oct-20	4.6	The installation procedure in BigBlueButton before 2.2.28 (or earlier) uses ClueCon as the FreeSWITCH password, which allows local users to achieve unintended FreeSWITCH access. **CVE ID : CVE-2020-27613**	N/A	A-BIG-BIGB-031120/119
greenlight					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Oct-20	4.3	A cross-site scripting (XSS) vulnerability exists in the 'merge account' functionality in admins.js in BigBlueButton Greenlight 2.7.6. **CVE ID : CVE-2020-27642**	N/A	A-BIG-GREE-031120/120

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
biscom					
secure_file_transfer					
Insufficiently Protected Credentials	22-Oct-20	4.3	Biscom Secure File Transfer (SFT) before 5.1.1082 and 6.x before 6.0.1011 allows user credential theft. **CVE ID : CVE-2020-27646**	N/A	A-BIS-SECU-031120/121
boltbrowser					
bolt_browser					
Missing Authentication for Critical Function	20-Oct-20	4.3	User Interface (UI) Misrepresentation of Critical Information vulnerability in the address bar of Danyil Vasilenko's Bolt Browser allows an attacker to obfuscate the true source of data as presented in the browser. This issue affects the Bolt Browser version 1.4 and prior versions. **CVE ID : CVE-2020-7370**	N/A	A-BOL-BOLT-031120/122
Checkpoint					
zonealarm					
N/A	27-Oct-20	3.6	Check Point ZoneAlarm before version 15.8.139.18543 allows a local actor to delete arbitrary files while restoring files in Anti-Ransomware. **CVE ID : CVE-2020-6022**	N/A	A-CHE-ZONE-031120/123
N/A	27-Oct-20	4.6	Check Point ZoneAlarm before version 15.8.139.18543 allows a local actor to escalate privileges while restoring files in Anti-Ransomware. **CVE ID : CVE-2020-6023**	N/A	A-CHE-ZONE-031120/124

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
chocolatey					
boxstarter					
Exposure of Resource to Wrong Sphere	20-Oct-20	7.2	The Boxstarter installer before version 2.13.0 configures C:\ProgramData\Boxstarter to be in the system-wide PATH environment variable. However, this directory is writable by normal, unprivileged users. To exploit the vulnerability, place a DLL in this directory that a privileged service is looking for. For example, WptsExtensions.dll When Windows starts, it'll execute the code in DllMain() with SYSTEM privileges. Any unprivileged user can execute code with SYSTEM privileges. The issue is fixed in version 3.13.0 **CVE ID : CVE-2020-15264**	https://github.com/chocolatey/boxstarter/security/advisories/GHSA-rpgx-h675-r3jf	A-CHO-BOXS-031120/125
Cisco					
cloud_services_router_1000v					
N/A	21-Oct-20	5	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured File Policy for HTTP. The vulnerability is due to incorrect detection of modified HTTP packets used in chunked responses. An attacker could exploit this vulnerability by sending	N/A	A-CIS-CLOU-031120/126

CVSS Scoring Scale	0-1	1-2	2-3	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 HTTP packets through an affected device. A successful exploit could allow the attacker to bypass a configured File Policy for HTTP packets and deliver a malicious payload. **CVE ID : CVE-2020-3299**		
isrv					
N/A	21-Oct-20	5	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured File Policy for HTTP. The vulnerability is due to incorrect detection of modified HTTP packets used in chunked responses. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass a configured File Policy for HTTP packets and deliver a malicious payload. **CVE ID : CVE-2020-3299**	N/A	A-CIS-ISRV-031120/127
adaptive_security_appliance					
Improper Neutralization of Special Elements used in an OS Command ('OS Command	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation	N/A	A-CIS-ADAP-031120/128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3457**		
N/A	21-Oct-20	4.6	Multiple vulnerabilities in the secure boot process of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software for the Firepower 1000 Series and Firepower 2100 Series Appliances could allow an authenticated, local attacker to bypass the secure boot mechanism. The vulnerabilities are due to insufficient protections of the secure boot process. An attacker could exploit these vulnerabilities by injecting code into specific files that are then referenced during the device boot process. A successful exploit could allow the attacker to break the chain of trust and inject code into the boot process of the device, which would be executed at each boot and maintain persistence across reboots.	N/A	A-CIS-ADAP-031120/129

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3458		
Improper Input Validation	21-Oct-20	7.8	A vulnerability in the web interface of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. The vulnerability is due to a lack of proper input validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. An exploit could allow the attacker to cause a DoS condition. Note: This vulnerability applies to IP Version 4 (IPv4) and IP Version 6 (IPv6) HTTP traffic. **CVE ID : CVE-2020-3304**	N/A	A-CIS-ADAP-031120/130
Improper Release of Memory Before Removing Last Reference	21-Oct-20	7.8	A vulnerability in the IP fragment-handling implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a memory leak on an affected device. This memory leak could prevent traffic from being processed through the device, resulting in a denial of service (DoS) condition. The	N/A	A-CIS-ADAP-031120/131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to improper error handling when specific failures occur during IP fragment reassembly. An attacker could exploit this vulnerability by sending crafted, fragmented IP traffic to a targeted device. A successful exploit could allow the attacker to continuously consume memory on the affected device and eventually impact traffic, resulting in a DoS condition. The device could require a manual reboot to recover from the DoS condition. Note: This vulnerability applies to both IP Version 4 (IPv4) and IP Version 6 (IPv6) traffic. **CVE ID : CVE-2020-3373**		
Unrestricted Upload of File with Dangerous Type	21-Oct-20	7.8	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to upload arbitrary-sized files to specific folders on an affected device, which could lead to an unexpected device reload. The vulnerability exists because the affected software does not efficiently handle the writing of large files to specific folders on the local file system. An attacker could exploit this vulnerability by	N/A	A-CIS-ADAP-031120/132

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
			uploading files to those specific folders. A successful exploit could allow the attacker to write a file that triggers a watchdog timeout, which would cause the device to unexpectedly reload, causing a denial of service (DoS) condition. **CVE ID : CVE-2020-3436**		
Uncontrolled Resource Consumption	21-Oct-20	5	A vulnerability in the OSPF Version 2 (OSPFv2) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. The vulnerability is due to incomplete input validation when the affected software processes certain OSPFv2 packets with Link-Local Signaling (LLS) data. An attacker could exploit this vulnerability by sending a malformed OSPFv2 packet to an affected device. A successful exploit could allow the attacker to cause an affected device to reload, resulting in a DoS condition. **CVE ID : CVE-2020-3528**	N/A	A-CIS-ADAP-031120/133
Uncontrolled Resource Consumption	21-Oct-20	5	A vulnerability in the SSL VPN negotiation process for Cisco Adaptive Security Appliance (ASA) Software	N/A	A-CIS-ADAP-031120/134

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to inefficient direct memory access (DMA) memory management during the negotiation phase of an SSL VPN connection. An attacker could exploit this vulnerability by sending a steady stream of crafted Datagram TLS (DTLS) traffic to an affected device. A successful exploit could allow the attacker to exhaust DMA memory on the device and cause a DoS condition. **CVE ID : CVE-2020-3529**		
Uncontrolled Resource Consumption	21-Oct-20	7.8	A vulnerability in the TCP packet processing of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to a memory exhaustion condition. An attacker could exploit this vulnerability by sending a high rate of crafted TCP traffic through an affected device. A successful exploit could allow the	N/A	A-CIS-ADAP-031120/135

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
			attacker to exhaust device resources, resulting in a DoS condition for traffic transiting the affected device. **CVE ID : CVE-2020-3554**		
Improper Resource Shutdown or Release	21-Oct-20	7.8	A vulnerability in the SIP inspection process of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a crash and reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a watchdog timeout and crash during the cleanup of threads that are associated with a SIP connection that is being deleted from the connection list. An attacker could exploit this vulnerability by sending a high rate of crafted SIP traffic through an affected device. A successful exploit could allow the attacker to cause a watchdog timeout and crash, resulting in a crash and reload of the affected device. **CVE ID : CVE-2020-3555**	N/A	A-CIS-ADAP-031120/136
Improper Neutralization of Special Elements in Output Used by a Downstream	21-Oct-20	4.3	A vulnerability in the Clientless SSL VPN (WebVPN) of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an	N/A	A-CIS-ADAP-031120/137

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Component ('Injection')			unauthenticated, remote attacker to inject arbitrary HTTP headers in the responses of the affected system. The vulnerability is due to improper input sanitization. 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 conduct a CRLF injection attack, adding arbitrary HTTP headers in the responses of the system and redirecting the user to arbitrary websites. **CVE ID : CVE-2020-3561**		
Improper Privilege Management	21-Oct-20	5	A vulnerability in the FTP inspection engine of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass FTP inspection. The vulnerability is due to ineffective flow tracking of FTP traffic. An attacker could exploit this vulnerability by sending crafted FTP traffic through an affected device. A successful exploit could allow the attacker to bypass FTP inspection and successfully complete FTP connections. **CVE ID : CVE-2020-3564**	N/A	A-CIS-ADAP-031120/138
Uncontrolled	21-Oct-20	5	A vulnerability in the	N/A	A-CIS-ADAP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource Consumption			SSL/TLS session handler of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to a memory leak when closing SSL/TLS connections in a specific state. An attacker could exploit this vulnerability by establishing several SSL/TLS sessions and ensuring they are closed under certain conditions. A successful exploit could allow the attacker to exhaust memory resources in the affected device, which would prevent it from processing new SSL/TLS connections, resulting in a DoS. Manual intervention is required to recover an affected device. **CVE ID : CVE-2020-3572**		031120/139
firepower_management_center					
Improper Authentication	21-Oct-20	6.8	A vulnerability in the Common Access Card (CAC) authentication feature of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to bypass authentication and access the FMC system. The attacker must have a valid CAC to	N/A	A-CIS-FIRE-031120/140

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			initiate the access attempt. The vulnerability is due to incorrect session invalidation during CAC authentication. An attacker could exploit this vulnerability by performing a CAC-based authentication attempt to an affected system. A successful exploit could allow the attacker to access an affected system with the privileges of a CAC-authenticated user who is currently logged in. **CVE ID : CVE-2020-3410**		
Uncontrolled Resource Consumption	21-Oct-20	5	A vulnerability in the licensing service of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.The vulnerability is due to improper handling of system resource values by the affected system. An attacker could exploit this vulnerability by sending malicious requests to the targeted system. A successful exploit could allow the attacker to cause the affected system to become unresponsive, resulting in a DoS condition and preventing the management of dependent devices. **CVE ID : CVE-2020-3499**	N/A	A-CIS-FIRE-031120/141
N/A	21-Oct-20	7.2	A vulnerability in the multi-instance feature of Cisco	N/A	A-CIS-FIRE-031120/142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their Cisco FTD instance and execute commands with root privileges in the host namespace. The attacker must have valid credentials on the device.The vulnerability exists because a configuration file that is used at container startup has insufficient protections. An attacker could exploit this vulnerability by modifying a specific container configuration file on the underlying file system. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running Cisco FTD instances or the host Cisco FXOS device. **CVE ID : CVE-2020-3514**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Oct-20	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker 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 by the	N/A	A-CIS-FIRE-031120/143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information. **CVE ID : CVE-2020-3515**		
Inadequate Encryption Strength	21-Oct-20	6.8	A vulnerability in the sftunnel functionality of Cisco Firepower Management Center (FMC) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to obtain the device registration hash. The vulnerability is due to insufficient sftunnel negotiation protection during initial device registration. An attacker in a man-in-the-middle position could exploit this vulnerability by intercepting a specific flow of the sftunnel communication between an FMC device and an FTD device. A successful exploit could allow the attacker to decrypt and modify the sftunnel communication between FMC and FTD devices, allowing the attacker to modify configuration data sent from an FMC device to an FTD	N/A	A-CIS-FIRE-031120/144

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device or alert data sent from an FTD device to an FMC device. **CVE ID : CVE-2020-3549**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Oct-20	5.5	A vulnerability in the sfmgr daemon of Cisco Firepower Management Center (FMC) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to perform directory traversal and access directories outside the restricted path. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by using a relative path in specific sfmgr commands. An exploit could allow the attacker to read or write arbitrary files on an sftunnel-connected peer device. **CVE ID : CVE-2020-3550**	N/A	A-CIS-FIRE-031120/145
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Oct-20	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker 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 by the web-based management interface. An attacker could	N/A	A-CIS-FIRE-031120/146

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information. **CVE ID : CVE-2020-3553**		
Improper Certificate Validation	21-Oct-20	5	A vulnerability in the host input API daemon of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper certificate validation. An attacker could exploit this vulnerability by sending a crafted data stream to the host input daemon of the affected device. A successful exploit could allow the attacker to cause the host input daemon to restart. The attacker could use repeated attacks to cause the daemon to continuously reload, creating a DoS condition for the API. **CVE ID : CVE-2020-3557**	N/A	A-CIS-FIRE-031120/147
URL Redirection to Untrusted Site ('Open Redirect')	21-Oct-20	5.8	A vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote	N/A	A-CIS-FIRE-031120/148

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting an HTTP request from a user. A successful exploit could allow the attacker to modify the HTTP request to cause the interface to redirect the user to a specific, malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2020-3558**		
firepower_threat_defense					
N/A	21-Oct-20	1.9	A vulnerability in the CLI of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to access hidden commands. The vulnerability is due to the presence of undocumented configuration commands. An attacker could exploit this vulnerability by performing specific steps that make the hidden commands accessible. A successful exploit could allow the attacker to make configuration changes to various sections of an affected device that should	N/A	A-CIS-FIRE-031120/149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			not be exposed to CLI access. **CVE ID : CVE-2020-3352**		
N/A	21-Oct-20	4.6	Multiple vulnerabilities in the secure boot process of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software for the Firepower 1000 Series and Firepower 2100 Series Appliances could allow an authenticated, local attacker to bypass the secure boot mechanism. The vulnerabilities are due to insufficient protections of the secure boot process. An attacker could exploit these vulnerabilities by injecting code into specific files that are then referenced during the device boot process. A successful exploit could allow the attacker to break the chain of trust and inject code into the boot process of the device, which would be executed at each boot and maintain persistence across reboots. **CVE ID : CVE-2020-3458**	N/A	A-CIS-FIRE-031120/150
N/A	21-Oct-20	5	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured File Policy for HTTP. The vulnerability is due to incorrect detection of	N/A	A-CIS-FIRE-031120/151

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			modified HTTP packets used in chunked responses. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass a configured File Policy for HTTP packets and deliver a malicious payload. **CVE ID : CVE-2020-3299**		
Improper Input Validation	21-Oct-20	7.8	A vulnerability in the web interface of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. The vulnerability is due to a lack of proper input validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. An exploit could allow the attacker to cause a DoS condition. Note: This vulnerability applies to IP Version 4 (IPv4) and IP Version 6 (IPv6) HTTP traffic. **CVE ID : CVE-2020-3304**	N/A	A-CIS-FIRE-031120/152
Improper Input Validation	21-Oct-20	5	A vulnerability in the ssl_inspection component of Cisco Firepower Threat Defense (FTD) Software	N/A	A-CIS-FIRE-031120/153

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to crash Snort instances. The vulnerability is due to insufficient input validation in the ssl_inspection component. An attacker could exploit this vulnerability by sending a malformed TLS packet through a Cisco Adaptive Security Appliance (ASA). A successful exploit could allow the attacker to crash a Snort instance, resulting in a denial of service (DoS) condition. **CVE ID : CVE-2020-3317**		
Improper Release of Memory Before Removing Last Reference	21-Oct-20	7.8	A vulnerability in the IP fragment-handling implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a memory leak on an affected device. This memory leak could prevent traffic from being processed through the device, resulting in a denial of service (DoS) condition. The vulnerability is due to improper error handling when specific failures occur during IP fragment reassembly. An attacker could exploit this vulnerability by sending crafted, fragmented IP traffic to a targeted device. A	N/A	A-CIS-FIRE-031120/154

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to continuously consume memory on the affected device and eventually impact traffic, resulting in a DoS condition. The device could require a manual reboot to recover from the DoS condition. Note: This vulnerability applies to both IP Version 4 (IPv4) and IP Version 6 (IPv6) traffic. **CVE ID : CVE-2020-3373**		
Unrestricted Upload of File with Dangerous Type	21-Oct-20	7.8	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to upload arbitrary-sized files to specific folders on an affected device, which could lead to an unexpected device reload. The vulnerability exists because the affected software does not efficiently handle the writing of large files to specific folders on the local file system. An attacker could exploit this vulnerability by uploading files to those specific folders. A successful exploit could allow the attacker to write a file that triggers a watchdog timeout, which would cause the device to unexpectedly reload, causing a denial of service	N/A	A-CIS-FIRE-031120/155

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(DoS) condition. **CVE ID : CVE-2020-3436**		
N/A	21-Oct-20	7.2	A vulnerability in the multi-instance feature of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to escape the container for their Cisco FTD instance and execute commands with root privileges in the host namespace. The attacker must have valid credentials on the device.The vulnerability exists because a configuration file that is used at container startup has insufficient protections. An attacker could exploit this vulnerability by modifying a specific container configuration file on the underlying file system. A successful exploit could allow the attacker to execute commands with root privileges within the host namespace. This could allow the attacker to impact other running Cisco FTD instances or the host Cisco FXOS device. **CVE ID : CVE-2020-3514**	N/A	A-CIS-FIRE-031120/156
Uncontrolled Resource Consumption	21-Oct-20	5	A vulnerability in the OSPF Version 2 (OSPFv2) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow	N/A	A-CIS-FIRE-031120/157

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. The vulnerability is due to incomplete input validation when the affected software processes certain OSPFv2 packets with Link-Local Signaling (LLS) data. An attacker could exploit this vulnerability by sending a malformed OSPFv2 packet to an affected device. A successful exploit could allow the attacker to cause an affected device to reload, resulting in a DoS condition. **CVE ID : CVE-2020-3528**		
Uncontrolled Resource Consumption	21-Oct-20	5	A vulnerability in the SSL VPN negotiation process for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to inefficient direct memory access (DMA) memory management during the negotiation phase of an SSL VPN connection. An attacker could exploit this vulnerability by sending a steady stream of crafted Datagram TLS (DTLS) traffic to an affected device. A	N/A	A-CIS-FIRE-031120/158

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to exhaust DMA memory on the device and cause a DoS condition. **CVE ID : CVE-2020-3529**		
Uncontrolled Resource Consumption	21-Oct-20	5	A vulnerability in the Simple Network Management Protocol (SNMP) input packet processor of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to restart unexpectedly. The vulnerability is due to a lack of sufficient memory management protections under heavy SNMP polling loads. An attacker could exploit this vulnerability by sending a high rate of SNMP requests to the SNMP daemon through the management interface on an affected device. A successful exploit could allow the attacker to cause the SNMP daemon process to consume a large amount of system memory over time, which could then lead to an unexpected device restart, causing a denial of service (DoS) condition. This vulnerability affects all versions of SNMP. **CVE ID : CVE-2020-3533**	N/A	A-CIS-FIRE-031120/159
Inadequate Encryption	21-Oct-20	6.8	A vulnerability in the sftunnel functionality of Cisco	N/A	A-CIS-FIRE-031120/160

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Strength			Firepower Management Center (FMC) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to obtain the device registration hash. The vulnerability is due to insufficient sftunnel negotiation protection during initial device registration. An attacker in a man-in-the-middle position could exploit this vulnerability by intercepting a specific flow of the sftunnel communication between an FMC device and an FTD device. A successful exploit could allow the attacker to decrypt and modify the sftunnel communication between FMC and FTD devices, allowing the attacker to modify configuration data sent from an FMC device to an FTD device or alert data sent from an FTD device to an FMC device. **CVE ID : CVE-2020-3549**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Oct-20	5.5	A vulnerability in the sfmgr daemon of Cisco Firepower Management Center (FMC) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to perform directory traversal and access directories outside the	N/A	A-CIS-FIRE-031120/161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			restricted path. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by using a relative path in specific sfmgr commands. An exploit could allow the attacker to read or write arbitrary files on an sftunnel-connected peer device. **CVE ID : CVE-2020-3550**		
Uncontrolled Resource Consumption	21-Oct-20	7.8	A vulnerability in the TCP packet processing of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to a memory exhaustion condition. An attacker could exploit this vulnerability by sending a high rate of crafted TCP traffic through an affected device. A successful exploit could allow the attacker to exhaust device resources, resulting in a DoS condition for traffic transiting the affected device. **CVE ID : CVE-2020-3554**	N/A	A-CIS-FIRE-031120/162
Improper Resource Shutdown or Release	21-Oct-20	7.8	A vulnerability in the SIP inspection process of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense	N/A	A-CIS-FIRE-031120/163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(FTD) Software could allow an unauthenticated, remote attacker to cause a crash and reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a watchdog timeout and crash during the cleanup of threads that are associated with a SIP connection that is being deleted from the connection list. An attacker could exploit this vulnerability by sending a high rate of crafted SIP traffic through an affected device. A successful exploit could allow the attacker to cause a watchdog timeout and crash, resulting in a crash and reload of the affected device. **CVE ID : CVE-2020-3555**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	21-Oct-20	4.3	A vulnerability in the Clientless SSL VPN (WebVPN) of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to inject arbitrary HTTP headers in the responses of the affected system. The vulnerability is due to improper input sanitization. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful	N/A	A-CIS-FIRE-031120/164

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to conduct a CRLF injection attack, adding arbitrary HTTP headers in the responses of the system and redirecting the user to arbitrary websites. **CVE ID : CVE-2020-3561**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-Oct-20	7.1	A vulnerability in the SSL/TLS inspection of Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 2100 Series firewalls could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper input validation for certain fields of specific SSL/TLS messages. An attacker could exploit this vulnerability by sending a malformed SSL/TLS message through an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. No manual intervention is needed to recover the device after it has reloaded. **CVE ID : CVE-2020-3562**	N/A	A-CIS-FIRE-031120/165
Uncontrolled Resource Consumption	21-Oct-20	7.8	A vulnerability in the packet processing functionality of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote	N/A	A-CIS-FIRE-031120/166

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to inefficient memory management. An attacker could exploit this vulnerability by sending a large number of TCP packets to a specific port on an affected device. A successful exploit could allow the attacker to exhaust system memory, which could cause the device to reload unexpectedly. No manual intervention is needed to recover the device after it has reloaded. **CVE ID : CVE-2020-3563**		
Improper Privilege Management	21-Oct-20	5	A vulnerability in the FTP inspection engine of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass FTP inspection. The vulnerability is due to ineffective flow tracking of FTP traffic. An attacker could exploit this vulnerability by sending crafted FTP traffic through an affected device. A successful exploit could allow the attacker to bypass FTP inspection and successfully complete FTP connections. **CVE ID : CVE-2020-3564**	N/A	A-CIS-FIRE-031120/167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authenticati on	21-Oct-20	4.3	A vulnerability in the TCP Intercept functionality of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass configured Access Control Policies (including Geolocation) and Service Polices on an affected system. The vulnerability exists because TCP Intercept is invoked when the embryonic connection limit is reached, which can cause the underlying detection engine to process the packet incorrectly. An attacker could exploit this vulnerability by sending a crafted stream of traffic that matches a policy on which TCP Intercept is configured. A successful exploit could allow the attacker to match on an incorrect policy, which could allow the traffic to be forwarded when it should be dropped. In addition, the traffic could incorrectly be dropped. **CVE ID : CVE-2020-3565**	N/A	A-CIS-FIRE-031120/168
Improper Input Validation	21-Oct-20	7.8	A vulnerability in the ICMP ingress packet processing of Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 4110 appliances could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an	N/A	A-CIS-FIRE-031120/169

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device. The vulnerability is due to incomplete input validation upon receiving ICMP packets. An attacker could exploit this vulnerability by sending a high number of crafted ICMP or ICMPv6 packets to an affected device. A successful exploit could allow the attacker to cause a memory exhaustion condition that may result in an unexpected reload. No manual intervention is needed to recover the device after the reload. **CVE ID : CVE-2020-3571**		
Uncontrolled Resource Consumption	21-Oct-20	5	A vulnerability in the SSL/TLS session handler of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to a memory leak when closing SSL/TLS connections in a specific state. An attacker could exploit this vulnerability by establishing several SSL/TLS sessions and ensuring they are closed under certain conditions. A successful exploit could allow the attacker to exhaust memory resources in the	N/A	A-CIS-FIRE-031120/170

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device, which would prevent it from processing new SSL/TLS connections, resulting in a DoS. Manual intervention is required to recover an affected device. **CVE ID : CVE-2020-3572**		
Improper Input Validation	21-Oct-20	6.1	A vulnerability in the ingress packet processing path of Cisco Firepower Threat Defense (FTD) Software for interfaces that are configured either as Inline Pair or in Passive mode could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition. The vulnerability is due to insufficient validation when Ethernet frames are processed. An attacker could exploit this vulnerability by sending malicious Ethernet frames through an affected device. A successful exploit could allow the attacker do either of the following: Fill the /ngfw partition on the device: A full /ngfw partition could result in administrators being unable to log in to the device (including logging in through the console port) or the device being unable to boot up correctly. Note: Manual intervention is required to recover from this situation. Customers are advised to contact the Cisco Technical Assistance Center (TAC) to help recover a	N/A	A-CIS-FIRE-031120/171

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device in this condition. Cause a process crash: The process crash would cause the device to reload. No manual intervention is necessary to recover the device after the reload. **CVE ID : CVE-2020-3577**		
clamxav					
clamxav					
Insufficient Verification of Data Authenticity	16-Oct-20	4.6	An issue was discovered in ClamXAV 3 before 3.1.1. A malicious actor could use a properly signed copy of ClamXAV 2 (running with an injected malicious dylib) to communicate with ClamXAV 3's helper tool and perform privileged operations. This occurs because of inadequate client verification in the helper tool. **CVE ID : CVE-2020-26893**	N/A	A-CLA-CLAM-031120/172
Cminds					
cm_download_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Oct-20	4.3	The cm-download-manager plugin before 2.8.0 for WordPress allows XSS. **CVE ID : CVE-2020-27344**	N/A	A-CMI-CM_D-031120/173
crmeb					
crmeb					
Server-Side Request Forgery	23-Oct-20	7.5	A SSRF vulnerability exists in the downloadimage interface of CRMEB 3.0, which can	N/A	A-CRM-CRME-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(SSRF)			remotely download arbitrary files on the server and remotely execute arbitrary code. **CVE ID : CVE-2020-25466**		031120/174
crossbeam_project					
crossbeam					
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Oct-20	7.5	Crossbeam is a set of tools for concurrent programming. In crossbeam-channel before version 0.4.4, the bounded channel incorrectly assumes that `Vec::from_iter` has allocated capacity that same as the number of iterator elements. `Vec::from_iter` does not actually guarantee that and may allocate extra memory. The destructor of the `bounded` channel reconstructs `Vec` from the raw pointer based on the incorrect assumes described above. This is unsound and causing deallocation with the incorrect capacity when `Vec::from_iter` has allocated different sizes with the number of iterator elements. This has been fixed in crossbeam-channel 0.4.4. **CVE ID : CVE-2020-15254**	https://github.com/crossbeam-rs/crossbeam/security/advisories/GHSA-v5m7-53cv-f3hx	A-CRO-CROS-031120/175
Dedecms					
dedecms					
Improper Neutralization of Input During Web Page	22-Oct-20	3.5	A Cross Site Scripting (XSS) issue was discovered in the search feature of DedeCMS v.5.8 that allows malicious users to inject code into web	N/A	A-DED-DEDE-031120/176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			pages, and other users will be affected when viewing web pages. **CVE ID : CVE-2020-27533**		
Dell					
emc_networker					
Files or Directories Accessible to External Parties	16-Oct-20	4	Dell EMC NetWorker versions prior to 19.3.0.2 contain an incorrect privilege assignment vulnerability. A non-LDAP remote user with low privileges may exploit this vulnerability to perform 'saveset' related operations in an unintended manner. The vulnerability is not exploitable by users authenticated via LDAP. **CVE ID : CVE-2020-26182**	https://www.dell.com/support/security/en-us/details/546616/DSA-2020-229-Dell-EMC-NetWorker-Multiple-Security-Vulnerabilities	A-DEL-EMC_-031120/177
Files or Directories Accessible to External Parties	16-Oct-20	4	Dell EMC NetWorker versions prior to 19.3.0.2 contain an improper authorization vulnerability. Certain remote users with low privileges may exploit this vulnerability to perform 'nsrmmdbd' operations in an unintended manner. **CVE ID : CVE-2020-26183**	https://www.dell.com/support/security/en-us/details/546616/DSA-2020-229-Dell-EMC-NetWorker-Multiple-Security-Vulnerabilities	A-DEL-EMC_-031120/178
eclecticiq					
opentaxii					
Server-Side Request Forgery (SSRF)	17-Oct-20	7.5	** DISPUTED ** TAXII libtaxii through 1.1.117, as used in EclecticIQ OpenTAXII through 0.2.0 and other	N/A	A-ECL-OPEN-031120/179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			products, allows SSRF via an initial http:// substring to the parse method, even when the no_network setting is used for the XML parser. NOTE: the vendor points out that the parse method "wraps the lxml library" and that this may be an issue to "raise ... to the lxml group." **CVE ID : CVE-2020-27197**		
eyoucms					
eyoucms					
Cross-Site Request Forgery (CSRF)	22-Oct-20	6.8	A CSRF vulnerability in Eyoucms v1.2.7 allows an attacker to add an admin account via login.php. **CVE ID : CVE-2020-18129**	N/A	A-EYO-EYOU-031120/180
fastd_project					
fastd					
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-Oct-20	5	receive.c in fastd before v21 allows denial of service (assertion failure) when receiving packets with an invalid type code. **CVE ID : CVE-2020-27638**	N/A	A-FAS-FAST-031120/181
fireeye					
email_malware_protection_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL	26-Oct-20	4	eMPS prior to eMPS 9.0 FireEye EX 3500 devices allows remote authenticated users to conduct SQL injection attacks via the sort, sort_by, search{URL], or search[attachment] parameter to the email	N/A	A-FIR-EMAI-031120/182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			search feature. **CVE ID : CVE-2020-25034**		
free					
freebox_server					
Authentication Bypass by Spoofing	19-Oct-20	4.3	A DNS rebinding vulnerability in the UPnP MediaServer implementation in Freebox Server before 4.2.3. **CVE ID : CVE-2020-24375**	https://dev.freebox.fr/blog/?p=10222	A-FRE-FREE-031120/183
fruitywifi_project					
fruitywifi					
Cross-Site Request Forgery (CSRF)	23-Oct-20	4.3	A Cross-Site Request Forgery (CSRF) vulnerability is identified in FruityWifi through 2.4. Due to a lack of CSRF protection in page_config_adv.php, an unauthenticated attacker can lure the victim to visit his website by social engineering or another attack vector. Due to this issue, an unauthenticated attacker can change the newSSID and hostapd_wpa_passphrase. **CVE ID : CVE-2020-24847**	N/A	A-FRU-FRUI-031120/184
Improper Privilege Management	23-Oct-20	7.2	FruityWifi through 2.4 has an unsafe Sudo configuration [(ALL : ALL) NOPASSWD: ALL]. This allows an attacker to perform a system-level (root) local privilege escalation, allowing an attacker to gain complete persistent access to the local system. **CVE ID : CVE-2020-24848**	N/A	A-FRU-FRUI-031120/185

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
getgophish					
gophish					
N/A	28-Oct-20	9.3	Gophish before 0.11.0 allows the creation of CSV sheets that contain malicious content. **CVE ID : CVE-2020-24707**	N/A	A-GET-GOPH-031120/186
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Oct-20	3.5	Cross Site Scripting (XSS) vulnerability in Gophish before 0.11.0 via the Host field on the send profile form. **CVE ID : CVE-2020-24708**	N/A	A-GET-GOPH-031120/187
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Oct-20	3.5	Cross Site Scripting (XSS) vulnerability in Gophish through 0.10.1 via a crafted landing page or email template. **CVE ID : CVE-2020-24709**	N/A	A-GET-GOPH-031120/188
Server-Side Request Forgery (SSRF)	28-Oct-20	5	Gophish before 0.11.0 allows SSRF attacks. **CVE ID : CVE-2020-24710**	N/A	A-GET-GOPH-031120/189
Improper Restriction of Rendered UI Layers or Frames	28-Oct-20	4.3	The Reset button on the Account Settings page in Gophish before 0.11.0 allows attackers to cause a denial of service via a clickjacking attack **CVE ID : CVE-2020-24711**	N/A	A-GET-GOPH-031120/190
Improper Neutralization of Input During Web	28-Oct-20	3.5	Cross Site Scripting (XSS) vulnerability in Gophish before 0.11.0 via the IMAP Host field on the account	N/A	A-GET-GOPH-031120/191

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			settings page. **CVE ID : CVE-2020-24712**		
Insufficient Session Expiration	28-Oct-20	5	Gophish through 0.10.1 does not invalidate the gophish cookie upon logout. **CVE ID : CVE-2020-24713**	N/A	A-GET-GOPH-031120/192
Ghisler					
total_commander					
Incorrect Default Permissions	21-Oct-20	4.4	An issue was discovered in Ghisler Total Commander 9.51. Due to insufficient access restrictions in the default installation directory, an attacker can elevate privileges by replacing the %SYSTEMDRIVE%\totalcmd \TOTALCMD64.EXE binary. **CVE ID : CVE-2020-17381**	N/A	A-GHI-TOTA-031120/193
gitea					
gitea					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Oct-20	6.5	** DISPUTED ** The git hook feature in Gitea 1.1.0 through 1.12.5 allows for authenticated remote code execution. NOTE: The vendor has indicated this is not a vulnerability and states "This is a functionality of the software that is limited to a very limited subset of accounts. If you give someone the privilege to execute arbitrary code on your server, they can execute arbitrary code on your server. We provide very clear	N/A	A-GIT-GITE-031120/194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			warnings to users around this functionality and what it provides." **CVE ID : CVE-2020-14144**		
git-tag-annotation-action_project					
git-tag-annotation-action					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-Oct-20	6.5	In the git-tag-annotation-action (open source GitHub Action) before version 1.0.1, an attacker can execute arbitrary (*) shell commands if they can control the value of [the `tag` input] or manage to alter the value of [the `GITHUB_REF` environment variable]. The problem has been patched in version 1.0.1. If you don't use the `tag` input you are most likely safe. The `GITHUB_REF` environment variable is protected by the GitHub Actions environment so attacks from there should be impossible. If you must use the `tag` input and cannot upgrade to `> 1.0.0` make sure that the value is not controlled by another Action. **CVE ID : CVE-2020-15272**	https://github.com/ericcornelissen/git-tag-annotation-action/security/advisories/GHSA-hgx2-4pp9-357g	A-GIT-GIT--031120/195
gogs					
gogs					
Improper Neutralization of Special Elements used in an OS Command ('OS Command	16-Oct-20	6.5	The git hook feature in Gogs 0.5.5 through 0.12.2 allows for authenticated remote code execution. **CVE ID : CVE-2020-15867**	N/A	A-GOG-GOGS-031120/196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')					
Google					
tink					
N/A	19-Oct-20	5	A mis-handling of invalid unicode characters in the Java implementation of Tink versions prior to 1.5 allows an attacker to change the ID part of a ciphertext, which result in the creation of a second ciphertext that can decrypt to the same plaintext. This can be a problem with encrypting deterministic AEAD with a single key, and rely on a unique ciphertext-per-plaintext. **CVE ID : CVE-2020-8929**	https://github.com/google/tink/commit/93d839a5865b9d950dffdc9d0bc99b71280a8899, https://github.com/google/tink/security/advisories/GHSA-g5vf-v6wf-7w2r	A-GOO-TINK-031120/197
Gopro					
gpmf-parser					
Out-of-bounds Write	19-Oct-20	6.8	GoPro gpmf-parser through 1.5 has a stack out-of-bounds write vulnerability in GPMF_ExpandComplexTYPE(). Parsing malicious input can result in a crash or potentially arbitrary code execution. **CVE ID : CVE-2020-16158**	N/A	A-GOP-GPMF-031120/198
Out-of-bounds Read	19-Oct-20	6.4	GoPro gpmf-parser 1.5 has a heap out-of-bounds read and segfault in GPMF_ScaledData(). Parsing malicious input can result in a crash or information disclosure. **CVE ID : CVE-2020-16159**	N/A	A-GOP-GPMF-031120/199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Divide By Zero	19-Oct-20	5	GoPro gpmf-parser 1.5 has a division-by-zero vulnerability in GPMF_Decompress(). Parsing malicious input can result in a crash. **CVE ID : CVE-2020-16160**	N/A	A-GOP-GPMF-031120/200
Divide By Zero	19-Oct-20	5	GoPro gpmf-parser 1.5 has a division-by-zero vulnerability in GPMF_ScaledData(). Parsing malicious input can result in a crash. **CVE ID : CVE-2020-16161**	N/A	A-GOP-GPMF-031120/201
grafana					
grafana					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Oct-20	4.3	Grafana before 7.1.0-beta 1 allows XSS via a query alias for the ElasticSearch datasource. **CVE ID : CVE-2020-24303**	N/A	A-GRA-GRAF-031120/202
halgatewood					
testimonial_rotator					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-20	3.5	Testimonial Rotator Wordpress Plugin 3.0.2 is affected by Cross Site Scripting (XSS) in /wp-admin/post.php. If a user intercepts a request and inserts a payload in "cite" parameter, the payload will be stored in the database. **CVE ID : CVE-2020-26672**	N/A	A-HAL-TEST-031120/203
HP					
bluedata_epic					
Insufficiently	26-Oct-20	4	The HPE BlueData EPIC	N/A	A-HP-BLUE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Software Platform version 4.0 and HPE Ezmeral Container Platform 5.0 use an insecure method of handling sensitive Kerberos passwords that is susceptible to unauthorized interception and/or retrieval. Specifically, they display the kdc_admin_password in the source file of the url "/bdswebui/assignusers/". **CVE ID : CVE-2020-7196**		031120/204
ezmeral_container_platform					
Insufficiently Protected Credentials	26-Oct-20	4	The HPE BlueData EPIC Software Platform version 4.0 and HPE Ezmeral Container Platform 5.0 use an insecure method of handling sensitive Kerberos passwords that is susceptible to unauthorized interception and/or retrieval. Specifically, they display the kdc_admin_password in the source file of the url "/bdswebui/assignusers/". **CVE ID : CVE-2020-7196**	N/A	A-HP-EZME-031120/205
intelligent_management_center					
Improper Authentication	19-Oct-20	10	A remote urlaccesscontroller authentication bypass vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-24629**	N/A	A-HP-INTE-031120/206
Improper Privilege Management	19-Oct-20	9	A remote operatoronlinelist_content privilege escalation vulnerability was discovered	N/A	A-HP-INTE-031120/207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-24630**		
Out-of-bounds Write	19-Oct-20	10	A tftpserver stack-based buffer overflow remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-24646**	N/A	A-HP-INTE-031120/208
Improper Input Validation	19-Oct-20	10	A remote accessmgrservlet classname input validation code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-24647**	N/A	A-HP-INTE-031120/209
Deserialization of Untrusted Data	19-Oct-20	10	A accessmgrservlet classname deserialization of untrusted data remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-24648**	N/A	A-HP-INTE-031120/210
Improper Input Validation	19-Oct-20	10	A remote bytemessageresource transformentity" input validation code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT	N/A	A-HP-INTE-031120/211

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			7.3 (E0705P07). **CVE ID : CVE-2020-24649**		
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	9	A powershellconfigcontent expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7186**	N/A	A-HP-INTE-031120/212
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	9	A reportpage index expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7187**	N/A	A-HP-INTE-031120/213
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	9	A userselectpagingcontent expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7188**	N/A	A-HP-INTE-031120/214
Improper Neutralization of Special Elements used in an	19-Oct-20	9	A faultflasheventselectfact expression language injectionremote code execution vulnerability was discovered in HPE Intelligent	N/A	A-HP-INTE-031120/215

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Expression Language Statement ('Expression Language Injection')			Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7189**		
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	9	A deviceselect expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7190**	N/A	A-HP-INTE-031120/216
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	9	A devsoftsel expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7191**	N/A	A-HP-INTE-031120/217
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	9	A devicethresholdconfig expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7192**	N/A	A-HP-INTE-031120/218
Improper	19-Oct-20	9	A ictexpertcsvdownload	N/A	A-HP-INTE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')			expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7193**		031120/219
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	9	A perfaddormoddevicemonitor expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7194**	N/A	A-HP-INTE-031120/220
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	9	A iccselectrules expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7195**	N/A	A-HP-INTE-031120/221
Improper Neutralization of Special Elements used in an Expression Language Statement	19-Oct-20	10	A legend expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-24650**	N/A	A-HP-INTE-031120/222

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Expression Language Injection')					
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	10	A syslogtempletselectwin expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-24651**	N/A	A-HP-INTE-031120/223
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	10	A addvsiinterfaceinfo expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-24652**	N/A	A-HP-INTE-031120/224
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	10	A adddevicetoview expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7141**	N/A	A-HP-INTE-031120/225
Improper Neutralization of Special Elements	19-Oct-20	10	A eventinfo_content expression language injection remote code execution vulnerability was discovered	N/A	A-HP-INTE-031120/226

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an Expression Language Statement ('Expression Language Injection')			in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7142**		
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	10	A faultdevparasset expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7143**	N/A	A-HP-INTE-031120/227
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	10	A comparefilesresult expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7144**	N/A	A-HP-INTE-031120/228
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	10	A chooseperfview expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7145**	N/A	A-HP-INTE-031120/229

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	10	A devgroupselect expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7146**	N/A	A-HP-INTE-031120/230
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	10	A deployselectbootrom expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7147**	N/A	A-HP-INTE-031120/231
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	10	A deployselectsoftware expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7148**	N/A	A-HP-INTE-031120/232
Improper Neutralization of Special Elements used in an Expression Language	19-Oct-20	10	A ictexpertcsvdownload expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT	N/A	A-HP-INTE-031120/233

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Statement ('Expression Language Injection')			7.3 (E0705P07). **CVE ID : CVE-2020-7149**		
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	10	A faultstatchoosefaulttype expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7150**	N/A	A-HP-INTE-031120/234
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	10	A faulttrapgroupselect expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7151**	N/A	A-HP-INTE-031120/235
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	10	A faultparasset expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7152**	N/A	A-HP-INTE-031120/236
Improper Neutralization of Special	19-Oct-20	10	A iccselectdevtype expression language injection remote code execution vulnerability	N/A	A-HP-INTE-031120/237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an Expression Language Statement ('Expression Language Injection')			was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7153**		
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	10	A ifviewselectpage expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7154**	N/A	A-HP-INTE-031120/238
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	10	A select expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7155**	N/A	A-HP-INTE-031120/239
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language	19-Oct-20	10	A faultinfo_content expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7156**	N/A	A-HP-INTE-031120/240

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')					
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	10	A selviewnavcontent expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7157**	N/A	A-HP-INTE-031120/241
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	10	A perfselecttask expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7158**	N/A	A-HP-INTE-031120/242
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	10	A customtemplateselect expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7159**	N/A	A-HP-INTE-031120/243
Improper Neutralization of Special Elements used in an Expression	19-Oct-20	10	A iccselectdeviceseries expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC)	N/A	A-HP-INTE-031120/244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Language Statement ('Expression Language Injection')			version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7160**		
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	10	A reporttaskselect expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7161**	N/A	A-HP-INTE-031120/245
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	10	A operatorgroupselectcontent expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7162**	N/A	A-HP-INTE-031120/246
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	10	A navigationto expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7163**	N/A	A-HP-INTE-031120/247
Improper Neutralizatio	19-Oct-20	10	A operationselect expression language injection remote	N/A	A-HP-INTE-031120/248

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in an Expression Language Statement ('Expression Language Injection')			code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7164**		
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	10	A iccselectcommand expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7165**	N/A	A-HP-INTE-031120/249
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	10	A operatorgrouptreeselectcontent expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7166**	N/A	A-HP-INTE-031120/250
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression	19-Oct-20	10	A quicktemplateselect expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7167**	N/A	A-HP-INTE-031120/251

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Language Injection')					
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	10	A selectusergroup expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7168**	N/A	A-HP-INTE-031120/252
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	10	A ictexpertcsvdownload expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7169**	N/A	A-HP-INTE-031120/253
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	10	A select expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7170**	N/A	A-HP-INTE-031120/254
Improper Neutralization of Special Elements in Output Used	19-Oct-20	10	A guidatadetail expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management	N/A	A-HP-INTE-031120/255

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
by a Downstream Component ('Injection')			Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7171**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-Oct-20	10	A templateselect expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7172**	N/A	A-HP-INTE-031120/256
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	9	A actionselectcontent expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7173**	N/A	A-HP-INTE-031120/257
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	9	A soapconfigcontent expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7174**	N/A	A-HP-INTE-031120/258
Improper Neutralization of Special Elements used in an	19-Oct-20	9	A iccselectdymicparam expression language injection remote code execution vulnerability was discovered in HPE Intelligent	N/A	A-HP-INTE-031120/259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Expression Language Statement ('Expression Language Injection')			Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7175**		
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	9	A viewtaskresultdetailfact expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7176**	N/A	A-HP-INTE-031120/260
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	9	A wmiconfigcontent expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7177**	N/A	A-HP-INTE-031120/261
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	9	A mediaforaction expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7178**	N/A	A-HP-INTE-031120/262
Improper	19-Oct-20	9	A thirdpartyperfselecttask	N/A	A-HP-INTE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')			expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7179**		031120/263
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	9	A ictexpertdownload expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7180**	N/A	A-HP-INTE-031120/264
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	9	A smsrulesdownload expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7181**	N/A	A-HP-INTE-031120/265
Improper Neutralization of Special Elements used in an Expression Language Statement	19-Oct-20	9	A sshconfig expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7182**	N/A	A-HP-INTE-031120/266

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Expression Language Injection')					
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	9	A forwardredirect expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7183**	N/A	A-HP-INTE-031120/267
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	9	A viewbatchtaskresultdetailfact expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7184**	N/A	A-HP-INTE-031120/268
Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	19-Oct-20	9	A tvxlanlegend expression language injection remote code execution vulnerability was discovered in HPE Intelligent Management Center (iMC) version(s): Prior to iMC PLAT 7.3 (E0705P07). **CVE ID : CVE-2020-7185**	N/A	A-HP-INTE-031120/269
IBM					
i2_analysts_notebook					
Buffer Copy	29-Oct-20	9.3	IBM i2 Analyst Notebook	https://ww	A-IBM-I2_A-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			9.2.0 and 9.2.1 could allow a local attacker to execute arbitrary code on the system, caused by a memory corruption. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 187868. **CVE ID : CVE-2020-4721**	w.ibm.com/support/pages/node/6356497	031120/270
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Oct-20	9.3	IBM i2 Analyst Notebook 9.2.0 and 9.2.1 could allow a local attacker to execute arbitrary code on the system, caused by a memory corruption. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 187870. **CVE ID : CVE-2020-4722**	https://www.ibm.com/support/pages/node/6356497	A-IBM-I2_A-031120/271
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-Oct-20	9.3	IBM i2 Analyst Notebook 9.2.0 and 9.2.1 could allow a local attacker to execute arbitrary code on the system, caused by a memory corruption. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 187873. **CVE ID : CVE-2020-4723**	https://www.ibm.com/support/pages/node/6356497	A-IBM-I2_A-031120/272
Buffer Copy	29-Oct-20	9.3	IBM i2 Analyst Notebook	https://ww	A-IBM-I2_A-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			9.2.0 and 9.2.1 could allow a local attacker to execute arbitrary code on the system, caused by a memory corruption. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system. **CVE ID : CVE-2020-4724**	w.ibm.com/support/pages/node/6356497	031120/273
spectrum_scale					
Uncontrolled Resource Consumption	20-Oct-20	2.1	IBM Spectrum Scale V4.2.0.0 through V4.2.3.22 and V5.0.0.0 through V5.0.5 could allow a local attacker to cause a denial of service by sending a large number of RPC requests to the mmfsd daemon which would cause the service to crash. IBM X-Force ID: 181991. **CVE ID : CVE-2020-4491**	https://www.ibm.com/support/pages/node/6349465	A-IBM-SPEC-031120/274
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-20	4.3	IBM Spectrum Scale 5.0.0 through 5.0.5.2 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: 188517. **CVE ID : CVE-2020-4748**	https://www.ibm.com/support/pages/node/6349449	A-IBM-SPEC-031120/275
Reliance on Cookies without	20-Oct-20	4.3	IBM Spectrum Scale 5.0.0 through 5.0.5.2 does not set the secure attribute on	https://www.ibm.com/support/page	A-IBM-SPEC-031120/276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation and Integrity Checking			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: 188518. **CVE ID : CVE-2020-4749**	s/node/6349449	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-20	3.5	IBM Spectrum Scale 5.0.0 through 5.0.5.2 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: 188595. **CVE ID : CVE-2020-4755**	https://www.ibm.com/support/pages/node/6349449	A-IBM-SPEC-031120/277
Improper Resource Shutdown or Release	20-Oct-20	4.9	IBM Spectrum Scale V4.2.0.0 through V4.2.3.23 and V5.0.0.0 through V5.0.5.2 as well as IBM Elastic Storage System 6.0.0 through 6.0.1.0 could allow a local attacker to invoke a subset of ioctls on the device with invalid arguments that could crash the keneral and cause a denial of service. IBM X-Force ID: 188599. **CVE ID : CVE-2020-4756**	https://www.ibm.com/support/pages/node/6349469, https://www.ibm.com/support/pages/node/6349475	A-IBM-SPEC-031120/278

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sterling_file_gateway					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-20	3.5	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 6.0.3.1 and IBM Sterling File Gateway 2.2.0.0 through 6.0.3.1 are 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: 183933. **CVE ID : CVE-2020-4564**	https://www.ibm.com/support/pages/node/6349533, https://www.ibm.com/support/pages/node/6349539	A-IBM-STER-031120/279
security_guardium_big_data_intelligence					
Use of a Broken or Risky Cryptographic Algorithm	16-Oct-20	5	IBM Security Guardium Big Data Intelligence 1.0 (SonarG) uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 175560. **CVE ID : CVE-2020-4254**	https://www.ibm.com/support/pages/node/6348664	A-IBM-SECU-031120/280
elastic_storage_server					
Improper Resource Shutdown or Release	20-Oct-20	4.9	IBM Spectrum Scale V4.2.0.0 through V4.2.3.23 and V5.0.0.0 through V5.0.5.2 as well as IBM Elastic Storage System 6.0.0 through 6.0.1.0 could allow a local attacker to invoke a subset of ioctls on the device with invalid arguments that could crash the keneral and cause a denial of service. IBM X-Force	https://www.ibm.com/support/pages/node/6349469, https://www.ibm.com/support/pages/node/6349475	A-IBM-ELAS-031120/281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ID: 188599. **CVE ID : CVE-2020-4756**		
sterling_connect					
Out-of-bounds Read	28-Oct-20	5	IBM Sterling Connect Direct for Microsoft Windows 4.7, 4.8, 6.0, and 6.1 could allow a remote attacker to cause a denial of service, caused by a buffer over-read. Bysending a specially crafted request, the attacker could cause the application to crash. IBM X-Force ID: 188906. **CVE ID : CVE-2020-4767**	https://www.ibm.com/support/pages/node/6356019	A-IBM-STER-031120/282
i2_ibase					
Information Exposure Through an Error Message	30-Oct-20	5	IBM i2 iBase 8.9.13 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 184574. **CVE ID : CVE-2020-4584**	https://www.ibm.com/support/pages/node/6357065	A-IBM-I2_I-031120/283
Unrestricted Upload of File with Dangerous Type	30-Oct-20	6.8	IBM i2 iBase 8.9.13 could allow an attacker to upload arbitrary executable files which, when executed by an unsuspecting victim could result in code execution. IBM X-Force ID: 184579. **CVE ID : CVE-2020-4588**	https://www.ibm.com/support/pages/node/6357037	A-IBM-I2_I-031120/284
resilient_security_orchestration_automation_and_response					
Improper Neutralization of Special	16-Oct-20	6.5	IBM Resilient OnPrem 38.2 could allow a privileged user to inject malicious commands	https://www.ibm.com/support/page	A-IBM-RESI-031120/285

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			through Python3 scripting. IBM X-Force ID: 185503. **CVE ID : CVE-2020-4636**	s/node/6348694	
Authentication Bypass by Spoofing	29-Oct-20	3.3	IBM Resilient SOAR V38.0 could allow an attacker on the internal net work to provide the server with a spoofed source IP address. IBM X-Force ID: 190567. **CVE ID : CVE-2020-4864**	https://www.ibm.com/support/pages/node/6356441	A-IBM-RESI-031120/286
sterling_b2b_integrator					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-20	3.5	IBM Sterling B2B Integrator Standard Edition 5.2.0.0 through 6.0.3.1 and IBM Sterling File Gateway 2.2.0.0 through 6.0.3.1 are 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: 183933. **CVE ID : CVE-2020-4564**	https://www.ibm.com/support/pages/node/6349533, https://www.ibm.com/support/pages/node/6349539	A-IBM-STER-031120/287
websphere_application_server					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	28-Oct-20	4	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system.	https://www.ibm.com/support/pages/node/6356083	A-IBM-WEBS-031120/288

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-4782		
Imagemagick					
imagemagick					
Divide By Zero	22-Oct-20	4.3	ImageMagick 7.0.10-34 allows Division by Zero in OptimizeLayerFrames in MagickCore/layer.c, which may cause a denial of service. **CVE ID : CVE-2020-27560**	N/A	A-IMA-IMAG-031120/289
infinispan					
infinispan					
Missing Authorizatio n	19-Oct-20	5.6	A flaw was found in Infinispan version 10, where it permits local access to controls via both REST and HotRod APIs. This flaw allows a user authenticated to the local machine to perform all operations on the caches, including the creation, update, deletion, and shutdown of the entire server. **CVE ID : CVE-2020-10746**	N/A	A-INF-INFI-031120/290
Iobit					
malware_fighter					
N/A	27-Oct-20	6.9	An issue exits in IOBit Malware Fighter version 8.0.2.547. Local escalation of privileges is possible by dropping a malicious DLL file into the WindowsApps folder. **CVE ID : CVE-2020-23864**	N/A	A-IOB-MALW-031120/291
Jetbrains					
youtrack					
Server-Side	19-Oct-20	7.5	In JetBrains YouTrack before	https://blog.	A-JET-YOUT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Request Forgery (SSRF)			2020.2.10514, SSRF is possible because URL filtering can be escaped. **CVE ID : CVE-2020-15822**	jetbrains.com/blog/2020/08/06/jetbrains-security-bulletin-q2-2020/	031120/292
Juniper					
mist_cloud_ui					
Improper Authentication	16-Oct-20	4.3	When Security Assertion Markup Language (SAML) authentication is enabled, Juniper Networks Mist Cloud UI might incorrectly process invalid authentication certificates which could allow a malicious network-based user to access unauthorized data. This issue affects all Juniper Networks Mist Cloud UI versions prior to September 2 2020. **CVE ID : CVE-2020-1675**	https://kb.juniper.net/JSA11072	A-JUN-MIST-031120/293
Improper Handling of Exceptional Conditions	16-Oct-20	4.3	When SAML authentication is enabled, Juniper Networks Mist Cloud UI might incorrectly handle SAML responses, allowing a remote attacker to modify a valid SAML response without invalidating its cryptographic signature to bypass SAML authentication security controls. This issue affects all Juniper Networks Mist Cloud UI versions prior to September 2 2020. **CVE ID : CVE-2020-1676**	https://kb.juniper.net/JSA11072	A-JUN-MIST-031120/294
Improper	16-Oct-20	4.3	When SAML authentication is	https://kb.ju	A-JUN-MIST-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			enabled, Juniper Networks Mist Cloud UI might incorrectly handle child elements in SAML responses, allowing a remote attacker to modify a valid SAML response without invalidating its cryptographic signature to bypass SAML authentication security controls. This issue affects all Juniper Networks Mist Cloud UI versions prior to September 2 2020. **CVE ID : CVE-2020-1677**	niper.net/JSA11072	031120/295
vsrx					
Improper Input Validation	16-Oct-20	2.1	An input validation vulnerability exists in Juniper Networks Junos OS, allowing an attacker to crash the srxpfe process, causing a Denial of Service (DoS) through the use of specific maintenance commands. The srxpfe process restarts automatically, but continuous execution of the commands could lead to an extended Denial of Service condition. This issue only affects the SRX1500, SRX4100, SRX4200, NFX150, NFX250, and vSRX-based platforms. No other products or platforms are affected by this vulnerability. This issue affects Juniper Networks Junos OS: 15.1X49 versions prior to 15.1X49-D220 on SRX1500, SRX4100, SRX4200, vSRX; 17.4 versions prior to 17.4R3-S3 on	https://kb.juniper.net/JSA11079	A-JUN-VSRX-031120/296

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SRX1500, SRX4100, SRX4200, vSRX; 18.1 versions prior to 18.1R3-S11 on SRX1500, SRX4100, SRX4200, vSRX, NFX150; 18.2 versions prior to 18.2R3-S5 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 19.1 versions prior to 19.1R3-S2 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 19.2 versions prior to 19.2R1-S5, 19.2R3 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250. This issue does not affect Junos OS 19.3 or any subsequent version. **CVE ID : CVE-2020-1682**		
junos					
Improper Input Validation	16-Oct-20	5.8	The DHCPv6 Relay-Agent service, part of the Juniper Enhanced jdhcpd daemon shipped with Juniper Networks Junos OS has an Improper Input Validation vulnerability which will result in a Denial of Service (DoS) condition when a DHCPv6 client sends a specific DHPCv6 message allowing an attacker to	https://kb.juniper.net/JSA11049	A-JUN-JUNO-031120/297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially perform a Remote Code Execution (RCE) attack on the target device. Continuous receipt of the specific DHCPv6 client message will result in an extended Denial of Service (DoS) condition. If adjacent devices are also configured to relay DHCP packets, and are not affected by this issue and simply transparently forward unprocessed client DHCPv6 messages, then the attack vector can be a Network-based attack, instead of an Adjacent-device attack. No other DHCP services are affected. Receipt of the packet without configuration of the DHCPv6 Relay-Agent service, will not result in exploitability of this issue. This issue affects Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S15; 12.3X48 versions prior to 12.3X48-D95; 14.1X53 versions prior to 14.1X53-D53; 15.1 versions prior to 15.1R7-S6; 15.1X49 versions prior to 15.1X49-D200; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2; 17.2 versions prior to 17.2R3-S3; 17.2X75 versions prior to 17.2X75-D44; 17.3 versions		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R2-S6, 18.2R3-S2; 18.2X75 versions prior to 18.2X75-D12, 18.2X75-D33, 18.2X75-D435, 18.2X75-D60; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R3; 19.1 versions prior to 19.1R1-S4, 19.1R2; 19.2 versions prior to 19.2R1-S3, 19.2R2; 19.3 versions prior to 19.3R2. **CVE ID : CVE-2020-1656**		
Out-of-bounds Write	16-Oct-20	7.2	A stack buffer overflow vulnerability in the device control daemon (DCD) on Juniper Networks Junos OS allows a low privilege local user to create a Denial of Service (DoS) against the daemon or execute arbitrary code in the system with root privilege. This issue affects Juniper Networks Junos OS: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.2X75 versions prior to 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3-S4; 18.4 versions prior to 18.4R2-S5, 18.4R3-S5; 19.1 versions prior to	https://kb.juniper.net/JSA11061	A-JUN-JUNO-031120/298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.1R3-S3; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2-S2, 19.4R3; 20.1 versions prior to 20.1R1-S4, 20.1R2; 20.2 versions prior to 20.2R1-S1, 20.2R2. Versions of Junos OS prior to 17.3 are unaffected by this vulnerability. **CVE ID : CVE-2020-1664**		
N/A	16-Oct-20	5	On Juniper Networks MX Series and EX9200 Series, in a certain condition the IPv6 Distributed Denial of Service (DDoS) protection might not take affect when it reaches the threshold condition. The DDoS protection allows the device to continue to function while it is under DDoS attack, protecting both the Routing Engine (RE) and the Flexible PIC Concentrator (FPC) during the DDoS attack. When this issue occurs, the RE and/or the FPC can become overwhelmed, which could disrupt network protocol operations and/or interrupt traffic. This issue does not affect IPv4 DDoS protection. This issue affects MX Series and EX9200 Series with Trio-based PFEs (Packet Forwarding Engines). Please refer to https://kb.juniper.net/KB25385 for the list of Trio-based	https://kb.juniper.net/JSA11062	A-JUN-JUNO-031120/299

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PFEs. This issue affects Juniper Networks Junos OS on MX series and EX9200 Series: 17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R2-S7, 18.2R3, 18.2R3-S3; 18.2X75 versions prior to 18.2X75-D30; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2. **CVE ID : CVE-2020-1665**		
Uncontrolled Resource Consumption	16-Oct-20	3.3	On Juniper Networks EX2300 Series, receipt of a stream of specific multicast packets by the layer2 interface can cause high CPU load, which could lead to traffic interruption. This issue occurs when multicast packets are received by the layer 2 interface. To check if the device has high CPU load due to this issue, the administrator can issue the following command: user@host> show chassis routing-engine Routing Engine status: ... Idle 2 percent the "Idle" value shows as low (2 % in the example above), and also the following command: user@host> show system processes summary ... PID USERNAME PRI NICE SIZE RES STATE TIME WCPU	https://kb.juniper.net/JSA11065	A-JUN-JUNO-031120/300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			COMMAND 11639 root 52 0 283M 11296K select 12:15 44.97% eventd 11803 root 81 0 719M 239M RUN 251:12 31.98% fxpc{fxpc} the eventd and the fxpc processes might use higher WCPU percentage (respectively 44.97% and 31.98% in the above example). This issue affects Juniper Networks Junos OS on EX2300 Series: 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2. **CVE ID : CVE-2020-1668**		
Uncontrolled Resource Consumption	16-Oct-20	3.3	On Juniper Networks EX4300 Series, receipt of a stream of specific IPv4 packets can cause Routing Engine (RE) high CPU load, which could lead to network protocol operation issue and traffic interruption. This specific packets can originate only from within the broadcast domain where the device is connected. This issue occurs when the packets enter to the IRB interface. Only IPv4	N/A	A-JUN-JUNO-031120/301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			packets can trigger this issue. IPv6 packets cannot trigger this issue. This issue affects Juniper Networks Junos OS on EX4300 series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.1 versions prior to 18.1R3-S10; 18.2 versions prior to 18.2R3-S4; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2; 18.4 versions prior to 18.4R2-S4, 18.4R3-S2; 19.1 versions prior to 19.1R2-S2, 19.1R3-S1; 19.2 versions prior to 19.2R1-S5, 19.2R2-S1, 19.2R3; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2; 20.1 versions prior to 20.1R1-S3, 20.1R2. **CVE ID : CVE-2020-1670**		
N/A	16-Oct-20	5	On Juniper Networks Junos OS platforms configured as DHCPv6 local server or DHCPv6 Relay Agent, Juniper Networks Dynamic Host Configuration Protocol Daemon (JDHCPD) process might crash with a core dump if a malformed DHCPv6 packet is received, resulting with the restart of the daemon. This issue only affects DHCPv6, it does not affect DHCPv4. This issue affects: Juniper Networks Junos OS 17.4 versions prior to 17.4R2-S12, 17.4R3-S3;	https://kb.juniper.net/JSA11068	A-JUN-JUNO-031120/302

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.2X75 versions prior to 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.2 version 19.2R2 and later versions; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2-S2, 19.4R3; 20.1 versions prior to 20.1R1-S3, 20.1R2; This issue does not affect Juniper Networks Junos OS prior to 17.4R1. **CVE ID : CVE-2020-1671**		
Improper Input Validation	16-Oct-20	5	On Juniper Networks Junos OS devices configured with DHCPv6 relay enabled, receipt of a specific DHCPv6 packet might crash the jdhcpd daemon. The jdhcpd daemon automatically restarts without intervention, but continuous receipt of specific crafted DHCP messages will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. Only DHCPv6 packet can trigger this issue. DHCPv4 packet cannot trigger this issue. This issue affects Juniper Networks Junos OS: 17.3 versions prior to 17.3R3-S9;	https://kb.juniper.net/JSA11069	A-JUN-JUNO-031120/303

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			17.4 versions prior to 17.4R2-S11, 17.4R3-S2, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R2-S2, 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R2-S1, 19.2R3; 19.3 versions prior to 19.3R2-S4, 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S3, 20.1R2. **CVE ID : CVE-2020-1672**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-20	7.6	Insufficient Cross-Site Scripting (XSS) protection in Juniper Networks J-Web and web based (HTTP/HTTPS) services allows an unauthenticated attacker to hijack the target user's HTTP/HTTPS session and perform administrative actions on the Junos device as the targeted user. This issue only affects Juniper Networks Junos OS devices with HTTP/HTTPS services enabled such as J-Web, Web Authentication, Dynamic-VPN (DVPN), Firewall Authentication Pass-Through with Web-Redirect, and Zero Touch Provisioning (ZTP). Junos OS devices with HTTP/HTTPS services	https://kb.juniper.net/JSA11070	A-JUN-JUNO-031120/304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disabled are not affected. If HTTP/HTTPS services are enabled, the following command will show the httpd processes: user@device> show system processes | match http 5260 - S 0:00.13 /usr/sbin/httpd-gk -N 5797 - I 0:00.10 /usr/sbin/httpd --config /jail/var/etc/httpd.conf In order to successfully exploit this vulnerability, the attacker needs to convince the device administrator to take action such as clicking the crafted URL sent via phishing email or convince the administrator to input data in the browser console. This issue affects Juniper Networks Junos OS: 18.1 versions prior to 18.1R3-S1; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2; 18.4 versions prior to 18.4R2-S5, 18.4R3-S2; 19.1 versions prior to 19.1R2-S2, 19.1R3-S1; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2; 20.1 versions prior to 20.1R1-S2, 20.1R2. This issue does not affect Juniper Networks Junos OS prior to 18.1R1. **CVE ID : CVE-2020-1673**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Oct-20	4.3	On Juniper Networks PTX and QFX Series devices with packet sampling configured using tunnel-observation mpls-over-udp, sampling of a malformed packet can cause the Kernel Routing Table (KRT) queue to become stuck. KRT is the module within the Routing Process Daemon (RPD) that synchronized the routing tables with the forwarding tables in the kernel. This table is then synchronized to the Packet Forwarding Engine (PFE) via the KRT queue. Thus, when KRT queue become stuck, it can lead to unexpected packet forwarding issues. An administrator can monitor the following command to check if there is the KRT queue is stuck: user@device > show krt state ... Number of async queue entries: 65007 <--- this value keep on increasing. When this issue occurs, the following message might appear in the /var/log/messages: DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Too many delayed route/nexthop unrefs. Op 2 err 55, rtsm_id 5:-1, msg type 2 DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Memory usage of M_RTNEXTHOP type = (0) Max size possible for	https://kb.juniper.net/JSA11076	A-JUN-JUNO-031120/305

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			M_RTNEXTHOP type = (7297134592) Current delayed unref = (60000), Current unique delayed unref = (18420), Max delayed unref on this platform = (40000) Current delayed weight unref = (60000) Max delayed weight unref on this platform= (400000) curproc = rpd This issue affects Juniper Networks Junos OS on PTX/QFX Series: 17.2X75 versions prior to 17.2X75-D105; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.2X75 versions prior to 18.2X75-D420, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R1-S7, 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R2-S2, 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2. This issue does not affect Juniper Networks Junos OS prior to 18.1R1. **CVE ID : CVE-2020-1679**		
Incorrect Calculation of Buffer Size	16-Oct-20	5	On Juniper Networks MX Series with MS-MIC or MS-MPC card configured with NAT64 configuration, receipt of a malformed IPv6 packet may crash the MS-PIC	https://kb.juniper.net/JSA11077	A-JUN-JUNO-031120/306

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			component on MS-MIC or MS-MPC. This issue occurs when a multiservice card is translating the malformed IPv6 packet to IPv4 packet. An unauthenticated attacker can continuously send crafted IPv6 packets through the device causing repetitive MS-PIC process crashes, resulting in an extended Denial of Service condition. This issue affects Juniper Networks Junos OS on MX Series: 15.1 versions prior to 15.1R7-S7; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S6; 17.4 versions prior to 17.4R2-S11, 17.4R3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D430, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2. **CVE ID : CVE-2020-1680**		
Improper Input Validation	16-Oct-20	2.1	An input validation vulnerability exists in Juniper Networks Junos OS, allowing an attacker to crash the srxpfe process, causing a	https://kb.juniper.net/JSA11079	A-JUN-JUNO-031120/307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Denial of Service (DoS) through the use of specific maintenance commands. The srxpfe process restarts automatically, but continuous execution of the commands could lead to an extended Denial of Service condition. This issue only affects the SRX1500, SRX4100, SRX4200, NFX150, NFX250, and vSRX-based platforms. No other products or platforms are affected by this vulnerability. This issue affects Juniper Networks Junos OS: 15.1X49 versions prior to 15.1X49-D220 on SRX1500, SRX4100, SRX4200, vSRX; 17.4 versions prior to 17.4R3-S3 on SRX1500, SRX4100, SRX4200, vSRX; 18.1 versions prior to 18.1R3-S11 on SRX1500, SRX4100, SRX4200, vSRX, NFX150; 18.2 versions prior to 18.2R3-S5 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 19.1 versions prior to 19.1R3-S2 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 19.2 versions prior to 19.2R1-S5, 19.2R3 on		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250. This issue does not affect Junos OS 19.3 or any subsequent version. **CVE ID : CVE-2020-1682**		
Uncontrolled Resource Consumption	16-Oct-20	4.3	On Juniper Networks SRX Series configured with application identification inspection enabled, receipt of specific HTTP traffic can cause high CPU load utilization, which could lead to traffic interruption. Application identification is enabled by default and is automatically turned on when Intrusion Detection and Prevention (IDP), AppFW, AppQoS, or AppTrack is configured. Thus, this issue might occur when IDP, AppFW, AppQoS, or AppTrack is configured. This issue affects Juniper Networks Junos OS on SRX Series: 12.3X48 versions prior to 12.3X48-D105; 15.1X49 versions prior to 15.1X49-D221, 15.1X49-D230; 17.4 versions prior to 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S3; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2; 18.4 versions prior to 18.4R2-S5, 18.4R3-S1; 19.1 versions prior to 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3	https://kb.juniper.net/JSA11081	A-JUN-JUNO-031120/308

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 19.3R3; 19.4 versions prior to 19.4R2. **CVE ID : CVE-2020-1684**		
Information Exposure Through Discrepancy	16-Oct-20	5	When configuring stateless firewall filters in Juniper Networks EX4600 and QFX 5000 Series devices using Virtual Extensible LAN protocol (VXLAN), the discard action will fail to discard traffic under certain conditions. Given a firewall filter configuration similar to: family ethernet-switching { filter L2-VLAN { term ALLOW { from { user-vlan-id 100; } then { accept; } } term NON-MATCH { then { discard; } } when there is only one term containing a 'user-vlan-id' match condition, and no other terms in the firewall filter except discard, the discard action for non-matching traffic will only discard traffic with the same VLAN ID specified under 'user-vlan-id'. Other traffic (e.g. VLAN ID 200) will not be discarded. This unexpected behavior can lead to unintended traffic passing through the interface where the firewall filter is applied. This issue only affects systems using VXLANs. This issue affects Juniper Networks Junos OS on QFX5K Series: 18.1 versions prior to 18.1R3-S7, except 18.1R3; 18.2 versions prior to	https://kb.juniper.net/JSA11082	A-JUN-JUNO-031120/309

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.2R2-S7, 18.2R3-S1; 18.3 versions prior to 18.3R1-S5, 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R1-S7, 18.4R2-S1, 18.4R3; 19.1 versions prior to 19.1R1-S5, 19.1R2; 19.2 versions prior to 19.2R1-S5, 19.2R2. **CVE ID : CVE-2020-1685**		
Missing Encryption of Sensitive Data	16-Oct-20	2.1	On Juniper Networks SRX Series and NFX Series, a local authenticated user with access to the shell may obtain the Web API service private key that is used to provide encrypted communication between the Juniper device and the authenticator services. Exploitation of this vulnerability may allow an attacker to decrypt the communications between the Juniper device and the authenticator service. This Web API service is used for authentication services such as the Juniper Identity Management Service, used to obtain user identity for Integrated User Firewall feature, or the integrated ClearPass authentication and enforcement feature. This issue affects Juniper Networks Junos OS on Networks SRX Series and NFX Series: 12.3X48 versions prior to 12.3X48-D105; 15.1X49 versions prior to 15.1X49-D190; 16.1 versions prior to 16.1R7-S8; 17.2	https://kb.juniper.net/JSA11085	A-JUN-JUNO-031120/310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3; 18.1 versions prior to 18.1R3-S7; 18.2 versions prior to 18.2R3; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R1-S7, 18.4R2; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S4, 19.2R2. **CVE ID : CVE-2020-1688**		
Uncontrolled Resource Consumption	16-Oct-20	3.3	On Juniper Networks EX4300-MP Series, EX4600 Series and QFX5K Series deployed in a Virtual Chassis configuration, receipt of a stream of specific layer 2 frames can cause high CPU load, which could lead to traffic interruption. This issue does not occur when the device is deployed in Stand Alone configuration. The offending layer 2 frame packets can originate only from within the broadcast domain where the device is connected. This issue affects Juniper Networks Junos OS on EX4300-MP Series, EX4600 Series and QFX5K Series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to	https://kb.juniper.net/JSA11086	A-JUN-JUNO-031120/311

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S3, 20.1R2. **CVE ID : CVE-2020-1689**		
KDE					
partition_manager					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	26-Oct-20	7.2	An issue was discovered in KDE Partition Manager 4.1.0 before 4.2.0. The kpmcore_externalcommand helper contains a logic flaw in which the service invoking D-Bus is not properly checked. An attacker on the local machine can replace /etc/fstab, and execute mount and other partitioning related commands, while KDE Partition Manager is running. the mount command can then be used to gain full root privileges. **CVE ID : CVE-2020-27187**	https://kde.org/info/security/advisory-20201017-1.txt	A-KDE-PART-031120/312
konzept-ix					
publixone					
Information Exposure	27-Oct-20	5	konzept-ix publiXone before 2020.015 allows attackers to download files by iterating over the IXCopy fileID parameter.	N/A	A-KON-PUBL-031120/313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-27180		
Inadequate Encryption Strength	27-Oct-20	6.4	A hardcoded AES key in CipherUtils.java in the Java applet of konzept-ix publiXone before 2020.015 allows attackers to craft password-reset tokens or decrypt server-side configuration files. **CVE ID : CVE-2020-27181**	N/A	A-KON-PUBL-031120/314
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-20	4.3	Multiple cross-site scripting (XSS) vulnerabilities in konzept-ix publiXone before 2020.015 allow remote attackers to inject arbitrary JavaScript or HTML via appletError.jsp, job_jacket_detail.jsp, ixedit/editor_component.jsp, or the login form. **CVE ID : CVE-2020-27182**	N/A	A-KON-PUBL-031120/315
Information Exposure	27-Oct-20	7.5	A RemoteFunctions endpoint with missing access control in konzept-ix publiXone before 2020.015 allows attackers to disclose sensitive user information, send arbitrary e-mails, escalate the privileges of arbitrary user accounts, and have unspecified other impact. **CVE ID : CVE-2020-27183**	N/A	A-KON-PUBL-031120/316
libass_project					
libass					
Integer Overflow or Wraparound	16-Oct-20	6.8	In libass 0.14.0, the `ass_outline_construct`'s call to `outline_stroke` causes a signed integer overflow.	N/A	A-LIB-LIBA-031120/317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-26682		
libtaxii_project					
libtaxii					
Server-Side Request Forgery (SSRF)	17-Oct-20	7.5	** DISPUTED ** TAXII libtaxii through 1.1.117, as used in EclecticIQ OpenTAXII through 0.2.0 and other products, allows SSRF via an initial http:// substring to the parse method, even when the no_network setting is used for the XML parser. NOTE: the vendor points out that the parse method "wraps the lxml library" and that this may be an issue to "raise ... to the lxml group." **CVE ID : CVE-2020-27197**	N/A	A-LIB-LIBT-031120/318
lightning_network_daemon_project					
lightning_network_daemon					
Improper Validation of Integrity Check Value	21-Oct-20	5	Prior to 0.10.0-beta, LND (Lightning Network Daemon) would have accepted a counterparty high-S signature and broadcast tx-relay invalid local commitment/HTLC transactions. This can be exploited by any peer with an open channel regardless of the victim situation (e.g., routing node, payment-receiver, or payment-sender). The impact is a loss of funds in certain situations. **CVE ID : CVE-2020-26895**	N/A	A-LIG-LIGH-031120/319
Improper Validation of	21-Oct-20	5.8	Prior to 0.11.0-beta, LND (Lightning Network Daemon)	N/A	A-LIG-LIGH-031120/320

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integrity Check Value			had a vulnerability in its invoice database. While claiming on-chain a received HTLC output, it didn't verify that the corresponding outgoing off-chain HTLC was already settled before releasing the preimage. In the case of a hash-and-amount collision with an invoice, the preimage for an expected payment was instead released. A malicious peer could have deliberately intercepted an HTLC intended for the victim node, probed the preimage through a colluding relayed HTLC, and stolen the intercepted HTLC. The impact is a loss of funds in certain situations, and a weakening of the victim's receiver privacy. **CVE ID : CVE-2020-26896**		
lightning-viz					
lightning					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-20	3.5	This affects all versions of package lightning-server. It is possible to inject malicious JavaScript code as part of a session controller. **CVE ID : CVE-2020-7747**	N/A	A-LIG-LIGH-031120/321
Linuxfoundation					
containerd					
Insufficiently Protected Credentials	16-Oct-20	4.3	In containerd (an industry-standard container runtime) before version 1.2.14 there is	https://github.com/containerd/contain	A-LIN-CONT-031120/322

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a credential leaking vulnerability. If a container image manifest in the OCI Image format or Docker Image V2 Schema 2 format includes a URL for the location of a specific image layer (otherwise known as a "foreign layer"), the default containerd resolver will follow that URL to attempt to download it. In v1.2.x but not 1.3.0 or later, the default containerd resolver will provide its authentication credentials if the server where the URL is located presents an HTTP 401 status code along with registry-specific HTTP headers. If an attacker publishes a public image with a manifest that directs one of the layers to be fetched from a web server they control and they trick a user or system into pulling the image, they can obtain the credentials used for pulling that image. In some cases, this may be the user's username and password for the registry. In other cases, this may be the credentials attached to the cloud virtual instance which can grant access to other cloud resources in the account. The default containerd resolver is used by the cri-containerd plugin (which can be used by Kubernetes), the ctr	erd/security /advisories/ GHSA-742w-89gc-8m9c	

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			development tool, and other client programs that have explicitly linked against it. This vulnerability has been fixed in containerd 1.2.14. containerd 1.3 and later are not affected. If you are using containerd 1.3 or later, you are not affected. If you are using cri-containerd in the 1.2 series or prior, you should ensure you only pull images from trusted sources. Other container runtimes built on top of containerd but not using the default resolver (such as Docker) are not affected. **CVE ID : CVE-2020-15157**		
loginizer					
loginizer					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Oct-20	7.5	The Loginizer plugin before 1.6.4 for WordPress allows SQL injection (with resultant XSS), related to loginizer_login_failed and lz_valid_ip. **CVE ID : CVE-2020-27615**	N/A	A-LOG-LOGI-031120/323
Magento					
magento					
Improper Neutralization of Input During Web Page Generation ('Cross-site	16-Oct-20	4.3	New description: Magento versions 2.4.0 and 2.3.5p2 (and earlier) are affected by a persistent XSS vulnerability that allows users to upload malicious JavaScript via the file upload component. This	N/A	A-MAG-MAGE-031120/324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			vulnerability could be abused by an unauthenticated attacker to execute XSS attacks against other Magento users. This vulnerability requires a victim to browse to the uploaded file. **CVE ID : CVE-2020-24408**		
marktext					
marktext					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-20	6.8	Mutation XSS exists in Mark Text through 0.16.2 that leads to Remote Code Execution. NOTE: this might be considered a duplicate of CVE-2020-26870; however, it can also be considered an issue in the design of the "source code mode" feature, which parses HTML even though HTML support is not one of the primary advertised roles of the product. **CVE ID : CVE-2020-27176**	N/A	A-MAR-MARK-031120/325
Matrix					
synapse					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-20	4.3	AuthRestServlet in Matrix Synapse before 1.21.0 is vulnerable to XSS due to unsafe interpolation of the session GET parameter. This allows a remote attacker to execute an XSS attack on the domain Synapse is hosted on, by supplying the victim user with a malicious URL to the /_matrix/client/r0/auth/*/fallback/web or	https://github.com/matrix-org/synapse/security/advisories/GHSA-3x8c-fmpc-5rmq	A-MAT-SYNA-031120/326

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			/_matrix/client/unstable/auth/*/fallback/web Synapse endpoints. **CVE ID : CVE-2020-26891**		
Mediawiki					
skin					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Oct-20	4.3	The Cosmos Skin for MediaWiki through 1.35.0 has stored XSS because MediaWiki messages were not being properly escaped. This is related to wfMessage and Html::rawElement, as demonstrated by CosmosSocialProfile::getUserGroups. **CVE ID : CVE-2020-27620**	N/A	A-MED-SKIN-031120/327
Microsoft					
365_apps					
N/A	16-Oct-20	9.3	A remote code execution vulnerability exists when the Base3D rendering engine 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 Base3D rendering engine handles memory., aka 'Base3D Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17003. **CVE ID : CVE-2020-16918**	N/A	A-MIC-365_-031120/328
Improper	16-Oct-20	6.8	An elevation of privilege	N/A	A-MIC-365_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			vulnerability exists in the way that Microsoft Office Click-to-Run (C2R) AppVLP handles certain files, aka 'Microsoft Office Click-to-Run Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16934, CVE-2020-16955. **CVE ID : CVE-2020-16928**		031120/329
Use After Free	16-Oct-20	6.8	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'. This CVE ID is unique from CVE-2020-16930, CVE-2020-16931, CVE-2020-16932. **CVE ID : CVE-2020-16929**	N/A	A-MIC-365_-031120/330
Out-of-bounds Write	16-Oct-20	6.8	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'. This CVE ID is unique from CVE-2020-16929, CVE-2020-16931, CVE-2020-16932. **CVE ID : CVE-2020-16930**	N/A	A-MIC-365_-031120/331
Use of Uninitialized Resource	16-Oct-20	6.8	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in	N/A	A-MIC-365_-031120/332

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-16929, CVE-2020-16930, CVE-2020-16932. **CVE ID : CVE-2020-16931**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Oct-20	6.8	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'. This CVE ID is unique from CVE-2020-16929, CVE-2020-16930, CVE-2020-16931. **CVE ID : CVE-2020-16932**	N/A	A-MIC-365_-031120/333
Improper Handling of Exceptional Conditions	16-Oct-20	6.8	A security feature bypass vulnerability exists in Microsoft Word software when it fails to properly handle .LNK files, aka 'Microsoft Word Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-16933**	N/A	A-MIC-365_-031120/334
Improper Privilege Management	16-Oct-20	6.8	An elevation of privilege vulnerability exists in the way that Microsoft Office Click-to-Run (C2R) AppVLP handles certain files, aka 'Microsoft Office Click-to-Run Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16928, CVE-2020-16955. **CVE ID : CVE-2020-16934**	N/A	A-MIC-365_-031120/335

CVSS Scoring Scale	0-1	1-2	2-3	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	16-Oct-20	9.3	A remote code execution vulnerability exists in Microsoft Outlook software when the software fails to properly handle objects in memory, aka 'Microsoft Outlook Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-16947**	N/A	A-MIC-365_-031120/336
Improper Release of Memory Before Removing Last Reference	16-Oct-20	5	A denial of service vulnerability exists in Microsoft Outlook software when the software fails to properly handle objects in memory, aka 'Microsoft Outlook Denial of Service Vulnerability'. **CVE ID : CVE-2020-16949**	N/A	A-MIC-365_-031120/337
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Oct-20	6.8	A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory, aka 'Microsoft Office Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-16954**	N/A	A-MIC-365_-031120/338
Improper Input Validation	16-Oct-20	6.8	An elevation of privilege vulnerability exists in the way that Microsoft Office Click-to-Run (C2R) AppVLP handles certain files, aka 'Microsoft Office Click-to-Run Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16928, CVE-2020-16934. **CVE ID : CVE-2020-16955**	N/A	A-MIC-365_-031120/339

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Oct-20	9.3	A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory, aka 'Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-16957**	N/A	A-MIC-365_-031120/340
sharepoint_designer					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-20	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-2020-16945. **CVE ID : CVE-2020-16946**	N/A	A-MIC-SHAR-031120/341
office_web_apps					
Use After Free	16-Oct-20	6.8	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'. This CVE ID is unique from CVE-2020-16930, CVE-2020-16931, CVE-2020-16932. **CVE ID : CVE-2020-16929**	N/A	A-MIC-OFFI-031120/342
Use of Uninitialized Resource	16-Oct-20	6.8	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to	N/A	A-MIC-OFFI-031120/343

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-16929, CVE-2020-16930, CVE-2020-16932. **CVE ID : CVE-2020-16931**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Oct-20	6.8	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'. This CVE ID is unique from CVE-2020-16929, CVE-2020-16930, CVE-2020-16931. **CVE ID : CVE-2020-16932**	N/A	A-MIC-OFFI-031120/344
powershellget					
N/A	16-Oct-20	7.2	A security feature bypass vulnerability exists in the PowerShellGet V2 module, aka 'PowerShellGet Module WDAC Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-16886**	N/A	A-MIC-POWE-031120/345
azure_functions					
Improper Privilege Management	16-Oct-20	7.5	An elevation of privilege vulnerability exists in the way Azure Functions validate access keys.An unauthenticated attacker who successfully exploited this vulnerability could invoke an HTTP Function without proper authorization.This security	N/A	A-MIC-AZUR-031120/346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			update addresses the vulnerability by correctly validating access keys used to access HTTP Functions., aka 'Azure Functions Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16904**		
3d_viewer					
N/A	16-Oct-20	9.3	A remote code execution vulnerability exists when the Base3D rendering engine 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 Base3D rendering engine handles memory., aka 'Base3D Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-17003. **CVE ID : CVE-2020-16918**	N/A	A-MIC-3D_V-031120/347
N/A	16-Oct-20	9.3	A remote code execution vulnerability exists when the Base3D rendering engine 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 Base3D rendering engine handles memory., aka 'Base3D Remote Code Execution	N/A	A-MIC-3D_V-031120/348

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. This CVE ID is unique from CVE-2020-16918. **CVE ID : CVE-2020-17003**		
excel_web_app					
Use After Free	16-Oct-20	6.8	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'. This CVE ID is unique from CVE-2020-16930, CVE-2020-16931, CVE-2020-16932. **CVE ID : CVE-2020-16929**	N/A	A-MIC-EXCE-031120/349
office_2013_click-to-run					
Improper Privilege Management	16-Oct-20	6.8	An elevation of privilege vulnerability exists in the way that Microsoft Office Click-to-Run (C2R) AppVLP handles certain files, aka 'Microsoft Office Click-to-Run Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16928, CVE-2020-16955. **CVE ID : CVE-2020-16934**	N/A	A-MIC-OFFI-031120/350
network_watcher_agent					
Improper Privilege Management	16-Oct-20	7.2	An elevation of privilege vulnerability exists in Network Watcher Agent virtual machine extension for Linux, aka 'Network Watcher Agent Virtual Machine Extension for Linux Elevation of Privilege Vulnerability'.	N/A	A-MIC-NETW-031120/351

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-16995		
office					
Improper Privilege Management	16-Oct-20	6.8	An elevation of privilege vulnerability exists in the way that Microsoft Office Click-to-Run (C2R) AppVLP handles certain files, aka 'Microsoft Office Click-to-Run Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16934, CVE-2020-16955. **CVE ID : CVE-2020-16928**	N/A	A-MIC-OFFI-031120/352
Use After Free	16-Oct-20	6.8	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'. This CVE ID is unique from CVE-2020-16930, CVE-2020-16931, CVE-2020-16932. **CVE ID : CVE-2020-16929**	N/A	A-MIC-OFFI-031120/353
Out-of-bounds Write	16-Oct-20	6.8	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'. This CVE ID is unique from CVE-2020-16929, CVE-2020-16931, CVE-2020-16932. **CVE ID : CVE-2020-16930**	N/A	A-MIC-OFFI-031120/354
Use of Uninitialized	16-Oct-20	6.8	A remote code execution vulnerability exists in	N/A	A-MIC-OFFI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource			Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-16929, CVE-2020-16930, CVE-2020-16932. **CVE ID : CVE-2020-16931**		031120/355
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Oct-20	6.8	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'. This CVE ID is unique from CVE-2020-16929, CVE-2020-16930, CVE-2020-16931. **CVE ID : CVE-2020-16932**	N/A	A-MIC-OFFI-031120/356
Improper Handling of Exceptional Conditions	16-Oct-20	6.8	A security feature bypass vulnerability exists in Microsoft Word software when it fails to properly handle .LNK files, aka 'Microsoft Word Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-16933**	N/A	A-MIC-OFFI-031120/357
Improper Privilege Management	16-Oct-20	6.8	An elevation of privilege vulnerability exists in the way that Microsoft Office Click-to-Run (C2R) AppVLP handles certain files, aka 'Microsoft Office Click-to-Run Elevation of Privilege Vulnerability'. This CVE ID is	N/A	A-MIC-OFFI-031120/358

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unique from CVE-2020-16928, CVE-2020-16955. **CVE ID : CVE-2020-16934**		
Out-of-bounds Write	16-Oct-20	9.3	A remote code execution vulnerability exists in Microsoft Outlook software when the software fails to properly handle objects in memory, aka 'Microsoft Outlook Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-16947**	N/A	A-MIC-OFFI-031120/359
Improper Release of Memory Before Removing Last Reference	16-Oct-20	5	A denial of service vulnerability exists in Microsoft Outlook software when the software fails to properly handle objects in memory, aka 'Microsoft Outlook Denial of Service Vulnerability'. **CVE ID : CVE-2020-16949**	N/A	A-MIC-OFFI-031120/360
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Oct-20	6.8	A remote code execution vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory, aka 'Microsoft Office Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-16954**	N/A	A-MIC-OFFI-031120/361
Improper Input Validation	16-Oct-20	6.8	An elevation of privilege vulnerability exists in the way that Microsoft Office Click-to-Run (C2R) AppVLP handles certain files, aka 'Microsoft Office Click-to-Run Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-	N/A	A-MIC-OFFI-031120/362

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			16928, CVE-2020-16934. **CVE ID : CVE-2020-16955**		
N/A	16-Oct-20	9.3	A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory, aka 'Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-16957**	N/A	A-MIC-OFFI-031120/363
.net_framework					
Information Exposure	16-Oct-20	4.3	An information disclosure vulnerability exists when the .NET Framework improperly handles objects in memory, aka '.NET Framework Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16937**	N/A	A-MIC-.NET-031120/364
sharepoint_server					
Use After Free	16-Oct-20	6.8	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'. This CVE ID is unique from CVE-2020-16930, CVE-2020-16931, CVE-2020-16932. **CVE ID : CVE-2020-16929**	N/A	A-MIC-SHAR-031120/365
Information Exposure	16-Oct-20	2.1	An information disclosure vulnerability exists when Microsoft SharePoint Server improperly discloses its	N/A	A-MIC-SHAR-031120/366

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			folder structure when rendering specific web pages, aka 'Microsoft SharePoint Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-16942, CVE-2020-16948, CVE-2020-16950, CVE-2020-16953. **CVE ID : CVE-2020-16941**		
Information Exposure	16-Oct-20	2.1	An information disclosure vulnerability exists when Microsoft SharePoint Server improperly discloses its folder structure when rendering specific web pages, aka 'Microsoft SharePoint Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-16941, CVE-2020-16948, CVE-2020-16950, CVE-2020-16953. **CVE ID : CVE-2020-16942**	N/A	A-MIC-SHAR-031120/367
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-20	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-2020-16944**	N/A	A-MIC-SHAR-031120/368
Improper Neutralizatio	16-Oct-20	3.5	A cross-site-scripting (XSS) vulnerability exists when	N/A	A-MIC-SHAR-031120/369

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			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-2020-16946. **CVE ID : CVE-2020-16945**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-20	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-2020-16945. **CVE ID : CVE-2020-16946**	N/A	A-MIC-SHAR-031120/370
N/A	16-Oct-20	4	An information disclosure vulnerability exists when Microsoft SharePoint Server fails to properly handle objects in memory, aka 'Microsoft SharePoint Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-16941, CVE-2020-16942, CVE-2020-16950, CVE-2020-16953. **CVE ID : CVE-2020-16948**	N/A	A-MIC-SHAR-031120/371
Information Exposure	16-Oct-20	4.3	An information disclosure vulnerability exists when Microsoft SharePoint Server fails to properly handle objects in memory, aka 'Microsoft SharePoint	N/A	A-MIC-SHAR-031120/372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-16941, CVE-2020-16942, CVE-2020-16948, CVE-2020-16953. **CVE ID : CVE-2020-16950**		
Origin Validation Error	16-Oct-20	6.8	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-16952. **CVE ID : CVE-2020-16951**	N/A	A-MIC-SHAR-031120/373
Origin Validation Error	16-Oct-20	6.8	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-16951. **CVE ID : CVE-2020-16952**	N/A	A-MIC-SHAR-031120/374
Information Exposure	16-Oct-20	4	An information disclosure vulnerability exists when Microsoft SharePoint Server fails to properly handle objects in memory, aka 'Microsoft SharePoint Information Disclosure Vulnerability'. This CVE ID is	N/A	A-MIC-SHAR-031120/375

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unique from CVE-2020-16941, CVE-2020-16942, CVE-2020-16948, CVE-2020-16950. **CVE ID : CVE-2020-16953**		
outlook					
Out-of-bounds Write	16-Oct-20	9.3	A remote code execution vulnerability exists in Microsoft Outlook software when the software fails to properly handle objects in memory, aka 'Microsoft Outlook Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-16947**	N/A	A-MIC-OUTL-031120/376
Improper Release of Memory Before Removing Last Reference	16-Oct-20	5	A denial of service vulnerability exists in Microsoft Outlook software when the software fails to properly handle objects in memory, aka 'Microsoft Outlook Denial of Service Vulnerability'. **CVE ID : CVE-2020-16949**	N/A	A-MIC-OUTL-031120/377
word					
Improper Handling of Exceptional Conditions	16-Oct-20	6.8	A security feature bypass vulnerability exists in Microsoft Word software when it fails to properly handle .LNK files, aka 'Microsoft Word Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-16933**	N/A	A-MIC-WORD-031120/378
sharepoint_enterprise_server					
Use After Free	16-Oct-20	6.8	A remote code execution vulnerability exists in Microsoft Excel software	N/A	A-MIC-SHAR-031120/379

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-16930, CVE-2020-16931, CVE-2020-16932. **CVE ID : CVE-2020-16929**		
Information Exposure	16-Oct-20	2.1	An information disclosure vulnerability exists when Microsoft SharePoint Server improperly discloses its folder structure when rendering specific web pages, aka 'Microsoft SharePoint Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-16942, CVE-2020-16948, CVE-2020-16950, CVE-2020-16953. **CVE ID : CVE-2020-16941**	N/A	A-MIC-SHAR-031120/380
Information Exposure	16-Oct-20	2.1	An information disclosure vulnerability exists when Microsoft SharePoint Server improperly discloses its folder structure when rendering specific web pages, aka 'Microsoft SharePoint Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-16941, CVE-2020-16948, CVE-2020-16950, CVE-2020-16953. **CVE ID : CVE-2020-16942**	N/A	A-MIC-SHAR-031120/381
Improper Neutralizatio	16-Oct-20	3.5	This vulnerability is caused when SharePoint Server does	N/A	A-MIC-SHAR-031120/382

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			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-2020-16944**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-20	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-2020-16946. **CVE ID : CVE-2020-16945**	N/A	A-MIC-SHAR-031120/383
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-20	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-2020-16945. **CVE ID : CVE-2020-16946**	N/A	A-MIC-SHAR-031120/384
N/A	16-Oct-20	4	An information disclosure vulnerability exists when Microsoft SharePoint Server fails to properly handle objects in memory, aka 'Microsoft SharePoint	N/A	A-MIC-SHAR-031120/385

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-16941, CVE-2020-16942, CVE-2020-16950, CVE-2020-16953. **CVE ID : CVE-2020-16948**		
Origin Validation Error	16-Oct-20	6.8	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-16952. **CVE ID : CVE-2020-16951**	N/A	A-MIC-SHAR-031120/386
Origin Validation Error	16-Oct-20	6.8	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-16951. **CVE ID : CVE-2020-16952**	N/A	A-MIC-SHAR-031120/387
Information Exposure	16-Oct-20	4	An information disclosure vulnerability exists when Microsoft SharePoint Server fails to properly handle objects in memory, aka 'Microsoft SharePoint Information Disclosure Vulnerability'. This CVE ID is	N/A	A-MIC-SHAR-031120/388

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unique from CVE-2020-16941, CVE-2020-16942, CVE-2020-16948, CVE-2020-16950. **CVE ID : CVE-2020-16953**		
office_online_server					
Use After Free	16-Oct-20	6.8	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'. This CVE ID is unique from CVE-2020-16930, CVE-2020-16931, CVE-2020-16932. **CVE ID : CVE-2020-16929**	N/A	A-MIC-OFFI-031120/389
Use of Uninitialized Resource	16-Oct-20	6.8	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'. This CVE ID is unique from CVE-2020-16929, CVE-2020-16930, CVE-2020-16932. **CVE ID : CVE-2020-16931**	N/A	A-MIC-OFFI-031120/390
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Oct-20	6.8	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'. This CVE ID is unique from CVE-2020-	N/A	A-MIC-OFFI-031120/391

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			16929, CVE-2020-16930, CVE-2020-16931. **CVE ID : CVE-2020-16932**		
exchange_server					
N/A	16-Oct-20	4.3	An information disclosure vulnerability exists in how Microsoft Exchange validates tokens when handling certain messages, aka 'Microsoft Exchange Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16969**	N/A	A-MIC-EXCH-031120/392
sharepoint_foundation					
Information Exposure	16-Oct-20	2.1	An information disclosure vulnerability exists when Microsoft SharePoint Server improperly discloses its folder structure when rendering specific web pages, aka 'Microsoft SharePoint Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-16942, CVE-2020-16948, CVE-2020-16950, CVE-2020-16953. **CVE ID : CVE-2020-16941**	N/A	A-MIC-SHAR-031120/393
Information Exposure	16-Oct-20	2.1	An information disclosure vulnerability exists when Microsoft SharePoint Server improperly discloses its folder structure when rendering specific web pages, aka 'Microsoft SharePoint Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-16941, CVE-2020-16948, CVE-2020-16950, CVE-2020-	N/A	A-MIC-SHAR-031120/394

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			16953. **CVE ID : CVE-2020-16942**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-20	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-2020-16944**	N/A	A-MIC-SHAR-031120/395
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-20	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-2020-16946. **CVE ID : CVE-2020-16945**	N/A	A-MIC-SHAR-031120/396
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-20	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-2020-16945. **CVE ID : CVE-2020-16946**	N/A	A-MIC-SHAR-031120/397
N/A	16-Oct-20	4	An information disclosure vulnerability exists when	N/A	A-MIC-SHAR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Microsoft SharePoint Server fails to properly handle objects in memory, aka 'Microsoft SharePoint Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-16941, CVE-2020-16942, CVE-2020-16950, CVE-2020-16953. **CVE ID : CVE-2020-16948**		031120/398
Origin Validation Error	16-Oct-20	6.8	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-16952. **CVE ID : CVE-2020-16951**	N/A	A-MIC-SHAR-031120/399
Origin Validation Error	16-Oct-20	6.8	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-16951. **CVE ID : CVE-2020-16952**	N/A	A-MIC-SHAR-031120/400
Information Exposure	16-Oct-20	4	An information disclosure vulnerability exists when Microsoft SharePoint Server fails to properly handle	N/A	A-MIC-SHAR-031120/401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			objects in memory, aka 'Microsoft SharePoint Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-16941, CVE-2020-16942, CVE-2020-16948, CVE-2020-16950. **CVE ID : CVE-2020-16953**		
excel					
Use After Free	16-Oct-20	6.8	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'. This CVE ID is unique from CVE-2020-16930, CVE-2020-16931, CVE-2020-16932. **CVE ID : CVE-2020-16929**	N/A	A-MIC-EXCE-031120/402
Use of Uninitialized Resource	16-Oct-20	6.8	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'. This CVE ID is unique from CVE-2020-16929, CVE-2020-16930, CVE-2020-16932. **CVE ID : CVE-2020-16931**	N/A	A-MIC-EXCE-031120/403
Improper Restriction of Operations within the	16-Oct-20	6.8	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in	N/A	A-MIC-EXCE-031120/404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-16929, CVE-2020-16930, CVE-2020-16931. **CVE ID : CVE-2020-16932**		
visual_studio_code					
N/A	16-Oct-20	9.3	A remote code execution vulnerability exists in Visual Studio Code when the Python extension loads a Jupyter notebook file, aka 'Visual Studio Code Python Extension Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-16977**	N/A	A-MIC-VISU-031120/405
N/A	16-Oct-20	9.3	A remote code execution vulnerability exists in Visual Studio Code when a user is tricked into opening a malicious 'package.json' file, aka 'Visual Studio JSON Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-17023**	N/A	A-MIC-VISU-031120/406
dynamics_365					
Incorrect Authorization	16-Oct-20	3.3	An elevation of privilege vulnerability exists in Microsoft Dynamics 365 Commerce, aka 'Dynamics 365 Commerce Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16943**	N/A	A-MIC-DYNA-031120/407
Improper Neutralization of Input During Web	16-Oct-20	3.5	A cross site scripting vulnerability exists when Microsoft Dynamics 365 (on-premises) does not properly	N/A	A-MIC-DYNA-031120/408

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			sanitize a specially crafted web request to an affected Dynamics server, aka 'Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability'. This CVE ID is unique from CVE-2020-16978. **CVE ID : CVE-2020-16956**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-20	3.5	A cross site scripting vulnerability exists when Microsoft Dynamics 365 (on-premises) does not properly sanitize a specially crafted web request to an affected Dynamics server, aka 'Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability'. This CVE ID is unique from CVE-2020-16956. **CVE ID : CVE-2020-16978**	N/A	A-MIC-DYNA-031120/409
mind					
imind_server					
Information Exposure	20-Oct-20	5	InterMind iMind Server through 3.13.65 allows remote unauthenticated attackers to read the self-diagnostic archive via a direct api/rs/monitoring/rs/api/system/dump-diagnostic-info?server=127.0.0.1 request. **CVE ID : CVE-2020-24765**	N/A	A-MIN-IMIN-031120/410
mintegral					
mintegraladsdk					
Improper Control of	19-Oct-20	10	This affects the package MintegralAdSDK before	N/A	A-MIN-MINT-031120/411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation of Code ('Code Injection')			6.6.0.0. The SDK distributed by the company contains malicious functionality that acts as a backdoor. Mintegral and their partners (advertisers) can remotely execute arbitrary code on a user device. **CVE ID : CVE-2020-7745**		
motion_project					
motion					
Out-of-bounds Read	26-Oct-20	5	A Denial of Service condition in Motion-Project Motion 3.2 through 4.3.1 allows remote unauthenticated users to cause a webu.c segmentation fault and kill the main process via a crafted HTTP request. **CVE ID : CVE-2020-26566**	N/A	A-MOT-MOTI-031120/412
Mozilla					
network_security_services					
Allocation of Resources Without Limits or Throttling	20-Oct-20	5	A flaw was found in the way NSS handled CCS (ChangeCipherSpec) messages in TLS 1.3. This flaw allows a remote attacker to send multiple CCS messages, causing a denial of service for servers compiled with the NSS library. The highest threat from this vulnerability is to system availability. This flaw affects NSS versions before 3.58. **CVE ID : CVE-2020-25648**	N/A	A-MOZ-NETW-031120/413
firefox					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	22-Oct-20	5	If a valid external protocol handler was referenced in an image tag, the resulting broken image size could be distinguished from a broken image size of a non-existent protocol handler. This allowed an attacker to successfully probe whether an external protocol handler was registered. This vulnerability affects Firefox < 82. **CVE ID : CVE-2020-15680**	N/A	A-MOZ-FIRE-031120/414
N/A	22-Oct-20	5	When multiple WASM threads had a reference to a module, and were looking up exported functions, one WASM thread could have overwritten another's entry in a shared stub table, resulting in a potentially exploitable crash. This vulnerability affects Firefox < 82. **CVE ID : CVE-2020-15681**	N/A	A-MOZ-FIRE-031120/415
Origin Validation Error	22-Oct-20	4.3	When a link to an external protocol was clicked, a prompt was presented that allowed the user to choose what application to open it in. An attacker could induce that prompt to be associated with an origin they didn't control, resulting in a spoofing attack. This was fixed by changing external protocol prompts to be tab-modal while also ensuring they could not be incorrectly associated with a	N/A	A-MOZ-FIRE-031120/416

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			different origin. This vulnerability affects Firefox < 82. **CVE ID : CVE-2020-15682**		
N/A	22-Oct-20	7.5	Mozilla developers and community members reported memory safety bugs present in Firefox 81 and Firefox ESR 78.3. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox ESR < 78.4, Firefox < 82, and Thunderbird < 78.4. **CVE ID : CVE-2020-15683**	N/A	A-MOZ-FIRE-031120/417
N/A	22-Oct-20	7.5	Mozilla developers reported memory safety bugs present in Firefox 81. 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 < 82. **CVE ID : CVE-2020-15684**	N/A	A-MOZ-FIRE-031120/418
firefox_esr					
N/A	22-Oct-20	7.5	Mozilla developers and community members reported memory safety bugs present in Firefox 81 and Firefox ESR 78.3. Some of these bugs showed evidence of memory corruption and we	N/A	A-MOZ-FIRE-031120/419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox ESR < 78.4, Firefox < 82, and Thunderbird < 78.4. **CVE ID : CVE-2020-15683**		
thunderbird					
N/A	22-Oct-20	7.5	Mozilla developers and community members reported memory safety bugs present in Firefox 81 and Firefox ESR 78.3. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox ESR < 78.4, Firefox < 82, and Thunderbird < 78.4. **CVE ID : CVE-2020-15683**	N/A	A-MOZ-THUN-031120/420
Nagios					
nagios_xi					
Cross-Site Request Forgery (CSRF)	20-Oct-20	4.3	Cross-site request forgery in Nagios XI 5.7.3 allows a remote attacker to perform sensitive application actions by tricking legitimate users into clicking a crafted link. **CVE ID : CVE-2020-5790**	N/A	A-NAG-NAGI-031120/421
Improper Neutralization of Special Elements used in an OS	20-Oct-20	9	Improper neutralization of special elements used in an OS command in Nagios XI 5.7.3 allows a remote, authenticated admin user to	N/A	A-NAG-NAGI-031120/422

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			execute operating system commands with the privileges of the apache user. **CVE ID : CVE-2020-5791**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Oct-20	6.5	Improper neutralization of argument delimiters in a command in Nagios XI 5.7.3 allows a remote, authenticated admin user to write to arbitrary files and ultimately execute code with the privileges of the apache user. **CVE ID : CVE-2020-5792**	N/A	A-NAG-NAGI-031120/423
neopost					
neopost_mail_accounting					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Oct-20	4.3	NeoPost Mail Accounting Software Pro 5.0.6 allows php/Commun/FUS_SCM_BlockStart.php?code= XSS. **CVE ID : CVE-2020-27974**	N/A	A-NEO-NEOP-031120/424
Netapp					
oncommand_insight					
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise	https://security.netapp.com/advisory/ntap-20201023-0003/	A-NET-ONCO-031120/425

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-2020-14672**		
N/A	21-Oct-20	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.21 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-2020-14800**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-NET-ONCO-031120/426
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 5.6.49 and	https://security.netapp.com/advisory/ntap-20201023-	A-NET-ONCO-031120/427

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior, 5.7.31 and prior and 8.0.21 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-2020-14765**	0003/	
N/A	21-Oct-20	3.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: LDAP Auth). Supported versions that are affected are 5.7.31 and prior and 8.0.21 and prior. Difficult to exploit 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 partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.2 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/	https://security.netapp.com/advisory/ntap-20201023-0003/	A-NET-ONCO-031120/428

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2020-14771**		
N/A	21-Oct-20	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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-2020-14773**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-NET-ONCO-031120/429
N/A	21-Oct-20	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.31 and prior and 8.0.21 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	https://security.netapp.com/advisory/ntap-20201023-0003/	A-NET-ONCO-031120/430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2020-14775**		
N/A	21-Oct-20	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.31 and prior and 8.0.21 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-2020-14776**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-NET-ONCO-031120/431
N/A	21-Oct-20	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access	https://security.netapp.com/advisory/ntap-20201023-0003/	A-NET-ONCO-031120/432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2020-14777**		
N/A	21-Oct-20	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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-2020-14785**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-NET-ONCO-031120/433
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server:	https://security.netapp.com/advisory	A-NET-ONCO-031120/434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Locking). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 8.0.21 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-2020-14812**	/ntap-20201023-0003/	
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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:	https://security.netapp.com/advisory/ntap-20201023-0003/	A-NET-ONCO-031120/435

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
			(CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14836**		
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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-2020-14837**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-NET-ONCO-031120/436
N/A	21-Oct-20	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.21 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	https://security.netapp.com/advisory/ntap-20201023-0003/	A-NET-ONCO-031120/437

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			read access to a subset of MySQL Server 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-2020-14838**		
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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-2020-14839**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-NET-ONCO-031120/438
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access	https://security.netapp.com/advisory/ntap-20201023-0003/	A-NET-ONCO-031120/439

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2020-14845**		
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Charsets). Supported versions that are affected are 8.0.21 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-2020-14852**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-NET-ONCO-031120/440
N/A	21-Oct-20	4.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster:	https://security.netapp.com/advisory	A-NET-ONCO-031120/441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NDBCluster Plugin). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 4.6 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:L). **CVE ID : CVE-2020-14853**	/ntap-20201023-0003/	
snapcenter					
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise	https://security.netapp.com/advisory/ntap-20201023-0003/	A-NET-SNAP-031120/442

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-2020-14672**		
N/A	21-Oct-20	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.21 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-2020-14800**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-NET-SNAP-031120/443
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 5.6.49 and	https://security.netapp.com/advisory/ntap-20201023-	A-NET-SNAP-031120/444

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior, 5.7.31 and prior and 8.0.21 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-2020-14765**	0003/	
N/A	21-Oct-20	3.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: LDAP Auth). Supported versions that are affected are 5.7.31 and prior and 8.0.21 and prior. Difficult to exploit 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 partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.2 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/	https://security.netapp.com/advisory/ntap-20201023-0003/	A-NET-SNAP-031120/445

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2020-14771**		
N/A	21-Oct-20	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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-2020-14773**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-NET-SNAP-031120/446
N/A	21-Oct-20	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.31 and prior and 8.0.21 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	https://security.netapp.com/advisory/ntap-20201023-0003/	A-NET-SNAP-031120/447

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2020-14775**		
N/A	21-Oct-20	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.31 and prior and 8.0.21 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-2020-14776**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-NET-SNAP-031120/448
N/A	21-Oct-20	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access	https://security.netapp.com/advisory/ntap-20201023-0003/	A-NET-SNAP-031120/449

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2020-14777**		
N/A	21-Oct-20	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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-2020-14785**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-NET-SNAP-031120/450
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server:	https://security.netapp.com/advisory	A-NET-SNAP-031120/451

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Locking). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 8.0.21 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-2020-14812**	/ntap-20201023-0003/	
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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:	https://security.netapp.com/advisory/ntap-20201023-0003/	A-NET-SNAP-031120/452

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
			(CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14836**		
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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-2020-14837**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-NET-SNAP-031120/453
N/A	21-Oct-20	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.21 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	https://security.netapp.com/advisory/ntap-20201023-0003/	A-NET-SNAP-031120/454

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			read access to a subset of MySQL Server 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-2020-14838**		
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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-2020-14839**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-NET-SNAP-031120/455
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access	https://security.netapp.com/advisory/ntap-20201023-0003/	A-NET-SNAP-031120/456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2020-14845**		
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Charsets). Supported versions that are affected are 8.0.21 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-2020-14852**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-NET-SNAP-031120/457
N/A	21-Oct-20	4.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster:	https://security.netapp.com/advisory	A-NET-SNAP-031120/458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NDBCluster Plugin). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 4.6 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:L). **CVE ID : CVE-2020-14853**	/ntap-20201023-0003/	
clustered_data_ontap					
N/A	27-Oct-20	5	Clustered Data ONTAP versions 9.7 through 9.7P7 are susceptible to a vulnerability which allows an attacker with access to an intercluster LIF to cause a Denial of Service (DoS). **CVE ID : CVE-2020-8579**	N/A	A-NET-CLUS-031120/459
netwrix					
account_lockout_examiner					
Authenticati	20-Oct-20	5	Netwrix Account Lockout	https://ww	A-NET-ACCO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on Bypass by Capture-replay			Examiner before 5.1 allows remote attackers to capture the Net-NTLMv1/v2 authentication challenge hash of the Domain Administrator (that is configured within the product in its installation state) by generating a single Kerberos Pre-Authentication Failed (ID 4771) event on a Domain Controller. **CVE ID : CVE-2020-15931**	w.netwrix.com/netwrix_reports_vulnerability_in_netwrix_account_lockout_examiner_4_1.html	031120/460
Npmjs					
npm-user-validate					
N/A	27-Oct-20	5	This affects the package npm-user-validate before 1.0.1. The regex that validates user emails took exponentially longer to process long input strings beginning with @ characters. **CVE ID : CVE-2020-7754**	https://github.com/npm/npm-user-validate/commit/c8a87dac1a4cc6988b5418f30411a8669bef204e, https://github.com/npm/npm-user-validate/security/advisories/GHSA-xgh6-85xh-479p, https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1019353	A-NPM-NPM--031120/461
Nvidia					
geforce_experience					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Search Path Element	23-Oct-20	4.4	NVIDIA GeForce Experience, all versions prior to 3.20.5.70, contains a vulnerability in NVIDIA Web Helper NodeJS Web Server in which an uncontrolled search path is used to load a node module, which may lead to code execution, denial of service, escalation of privileges, and information disclosure. **CVE ID : CVE-2020-5977**	https://nvidia.custhelp.com/app/answers/detail/a_id/5076	A-NVI-GEFO-031120/462
N/A	23-Oct-20	4.6	NVIDIA GeForce Experience, all versions prior to 3.20.5.70, contains a vulnerability in its services in which a folder is created by nvcontainer.exe under normal user login with LOCAL_SYSTEM privileges which may lead to a denial of service or escalation of privileges. **CVE ID : CVE-2020-5978**	https://nvidia.custhelp.com/app/answers/detail/a_id/5076	A-NVI-GEFO-031120/463
N/A	23-Oct-20	4.6	NVIDIA GeForce Experience, all versions prior to 3.20.5.70, contains a vulnerability in the ShadowPlay component which may lead to local privilege escalation, code execution, denial of service or information disclosure. **CVE ID : CVE-2020-5990**	https://nvidia.custhelp.com/app/answers/detail/a_id/5076	A-NVI-GEFO-031120/464
object-path_project					
object-path					
Improper Input Validation	19-Oct-20	6.8	A prototype pollution vulnerability has been found in `object-path` <= 0.11.4 affecting the `set()` method. The vulnerability is limited to	https://github.com/mariocasciaro/object-path/securit	A-OBJ-OBJE-031120/465

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the `includeInheritedProps` mode (if version >= 0.11.0 is used), which has to be explicitly enabled by creating a new instance of `object-path` and setting the option `includeInheritedProps: true`, or by using the default `withInheritedProps` instance. The default operating mode is not affected by the vulnerability if version >= 0.11.0 is used. Any usage of `set()` in versions < 0.11.0 is vulnerable. The issue is fixed in object-path version 0.11.5 As a workaround, don't use the `includeInheritedProps: true` options or the `withInheritedProps` instance if using a version >= 0.11.0. **CVE ID : CVE-2020-15256**	y/advisories /GHSA-cwx2-736x-mf6w	
octopus					
octopus_deploy					
N/A	22-Oct-20	4.3	An issue was discovered in Octopus Deploy through 2020.4.4. If enabled, the websocket endpoint may allow an untrusted tentacle host to present itself as a trusted one. **CVE ID : CVE-2020-27155**	N/A	A-OCT-OCTO-031120/466
URL Redirection to Untrusted Site ('Open Redirect')	26-Oct-20	5.8	In Octopus Deploy through 2020.4.2, an attacker could redirect users to an external site via a modified HTTP Host header.	N/A	A-OCT-OCTO-031120/467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-26161		
olimpoks					
olimpok					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-20	4.3	OLIMPOKS under 3.3.39 allows Auth/Admin ErrorMessage XSS. Remote Attacker can use discovered vulnerability to inject malicious JavaScript payload to victim's browsers in context of vulnerable applications. Executed code can be used to steal administrator's cookies, influence HTML content of targeted application and perform phishing-related attacks. Vulnerable application used in more than 3000 organizations in different sectors from retail to industries. **CVE ID : CVE-2020-16270**	N/A	A-OLI-OLIM-031120/468
Onethird					
onethird					
N/A	20-Oct-20	7.5	Local file inclusion vulnerability in OneThird CMS v1.96c and earlier allows a remote unauthenticated attacker to execute arbitrary code or obtain sensitive information via unspecified vectors. **CVE ID : CVE-2020-5640**	N/A	A-ONE-ONET-031120/469
Openstack					
blazar-dashboard					
N/A	16-Oct-20	9	An issue was discovered in OpenStack blazar-dashboard	https://security.openstac	A-OPE-BLAZ-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 1.3.1, 2.0.0, and 3.0.0. A user allowed to access the Blazar dashboard in Horizon may trigger code execution on the Horizon host as the user the Horizon service runs under (because the Python eval function is used). This may result in Horizon host unauthorized access and further compromise of the Horizon service. All setups using the Horizon dashboard with the blazar-dashboard plugin are affected. **CVE ID : CVE-2020-26943**	k.org/ossa/OSSA-2020-007.html	031120/470
Opensuse					
backports_sle					
N/A	16-Oct-20	5	An issue has been found in PowerDNS Recursor before 4.1.18, 4.2.x before 4.2.5, and 4.3.x before 4.3.5. A remote attacker can cause the cached records for a given name to be updated to the Bogus DNSSEC validation state, instead of their actual DNSSEC Secure state, via a DNS ANY query. This results in a denial of service for installation that always validate (dnssec=validate), and for clients requesting validation when on-demand validation is enabled (dnssec=process). **CVE ID : CVE-2020-25829**	https://docs.powerdns.com/recursor/security-advisories/powerdns-advisory-2020-07.html	A-OPE-BACK-031120/471
Open-xchange					
open-xchange_appsuite					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Server-Side Request Forgery (SSRF)	23-Oct-20	4	OX App Suite through 7.10.3 allows SSRF via the the /ajax/messaging/message message API. **CVE ID : CVE-2020-15002**	https://seclists.org/fulldisclosure/2020/Oct/20	A-OPE-OPEN-031120/472
Information Exposure	23-Oct-20	4	OX App Suite through 7.10.3 allows Information Exposure because a user can obtain the IP address and User-Agent string of a different user (via the session API during shared Drive access). **CVE ID : CVE-2020-15003**	https://seclists.org/fulldisclosure/2020/Oct/20	A-OPE-OPEN-031120/473
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Oct-20	3.5	OX App Suite through 7.10.3 allows stats/diagnostic?param= XSS. **CVE ID : CVE-2020-15004**	N/A	A-OPE-OPEN-031120/474
Oracle					
application_express					
N/A	21-Oct-20	4.9	Vulnerability in the Oracle Application Express component of Oracle Database Server. The supported version that is affected is Prior to 20.2. 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	N/A	A-ORA-APPL-031120/475

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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-2020-14762**		
N/A	21-Oct-20	4.9	Vulnerability in the Oracle Application Express Quick Poll component of Oracle Database Server. The supported version that is affected is Prior to 20.2. Easily exploitable vulnerability allows low privileged attacker having Valid User Account privilege with network access via HTTP to compromise Oracle Application Express Quick Poll. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Express Quick Poll, attacks may significantly impact additional products.	N/A	A-ORA-APPL-031120/476

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
			Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Express Quick Poll accessible data as well as unauthorized read access to a subset of Oracle Application Express Quick Poll 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-2020-14763**		
N/A	21-Oct-20	4.9	Vulnerability in the Oracle Application Express Packaged Apps component of Oracle Database Server. The supported version that is affected is Prior to 20.2. Easily exploitable vulnerability allows low privileged attacker having Valid User Account privilege with network access via HTTP to compromise Oracle Application Express Packaged Apps. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Express Packaged Apps, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert	N/A	A-ORA-APPL-031120/477

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			or delete access to some of Oracle Application Express Packaged Apps accessible data as well as unauthorized read access to a subset of Oracle Application Express Packaged Apps 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-2020-14898**		
N/A	21-Oct-20	4.9	Vulnerability in the Oracle Application Express Data Reporter component of Oracle Database Server. The supported version that is affected is Prior to 20.2. Easily exploitable vulnerability allows low privileged attacker having Valid User Account privilege with network access via HTTP to compromise Oracle Application Express Data Reporter. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Express Data Reporter, 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 Data Reporter accessible data	N/A	A-ORA-APPL-031120/478

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			as well as unauthorized read access to a subset of Oracle Application Express Data Reporter 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-2020-14899**		
N/A	21-Oct-20	4.9	Vulnerability in the Oracle Application Express Group Calendar component of Oracle Database Server. The supported version that is affected is Prior to 20.2. Easily exploitable vulnerability allows low privileged attacker having Valid User Account privilege with network access via HTTP to compromise Oracle Application Express Group Calendar. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Express Group Calendar, 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 Group Calendar accessible data as well as unauthorized read access to a subset of Oracle Application Express	N/A	A-ORA-APPL-031120/479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Group Calendar 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-2020-14900**		
universal_work_queue					
N/A	21-Oct-20	9	Vulnerability in the Oracle Universal Work Queue product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3 - 12.2.9. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Universal Work Queue. Successful attacks of this vulnerability can result in takeover of Oracle Universal Work Queue. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/ UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2020-14862**	N/A	A-ORA-UNIV-031120/480
N/A	21-Oct-20	10	Vulnerability in the Oracle Universal Work Queue product of Oracle E-Business Suite (component: Work Provider Administration). The supported version that is affected is 12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access	N/A	A-ORA-UNIV-031120/481

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via HTTP to compromise Oracle Universal Work Queue. Successful attacks of this vulnerability can result in takeover of Oracle Universal Work Queue. 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-2020-14855**		
customer_relationship_management_technical_foundation					
N/A	21-Oct-20	5	Vulnerability in the Oracle CRM Technical Foundation product of Oracle E-Business Suite (component: Preferences). Supported versions that are affected are 12.1.1 - 12.1.3 and 12.2.3 - 12.2.10. 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-2020-14774**	N/A	A-ORA-CUST-031120/482
N/A	21-Oct-20	5.5	Vulnerability in the Oracle CRM Technical Foundation	N/A	A-ORA-CUST-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			product of Oracle E-Business Suite (component: Preferences). Supported versions that are affected are 12.2.3 - 12.2.10. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle CRM Technical Foundation accessible data as well as unauthorized access to critical data or complete access to all Oracle CRM Technical Foundation accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2020-14823**		031120/483
N/A	21-Oct-20	7.8	Vulnerability in the Oracle CRM Technical Foundation product of Oracle E-Business Suite (component: Flex Fields). Supported versions that are affected are 12.1.3 and 12.2.3 - 12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical	N/A	A-ORA-CUST-031120/484

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, 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-2020-14850**		
peoplesoft_enterprise_scm_esupplier_connection					
N/A	21-Oct-20	8.5	Vulnerability in the PeopleSoft Enterprise SCM eSupplier Connection product of Oracle PeopleSoft (component: eSupplier Connection). 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 SCM eSupplier	N/A	A-ORA-PEOP-031120/485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connection. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise SCM eSupplier Connection accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise SCM eSupplier Connection 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-2020-14865**		
utilities_framework					
N/A	21-Oct-20	5.5	Vulnerability in the Oracle Utilities Framework product of Oracle Utilities Applications (component: System Wide). Supported versions that are affected are 2.2.0.0.0, 4.2.0.2.0, 4.2.0.3.0, 4.3.0.1.0 - 4.3.0.6.0, 4.4.0.0.0 and 4.4.0.2.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Utilities Framework. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Utilities Framework accessible data as well as	N/A	A-ORA-UTIL-031120/486

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized read access to a subset of Oracle Utilities Framework 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-2020-14895**		
text					
N/A	21-Oct-20	6.8	Vulnerability in the Oracle Text 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 unauthenticated attacker with network access via Oracle Net to compromise Oracle Text. Successful attacks of this vulnerability can result in takeover of Oracle Text. 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-2020-14734**	N/A	A-ORA-TEXT-031120/487
scheduler					
N/A	21-Oct-20	7.2	Vulnerability in the Scheduler 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. Easily exploitable vulnerability allows low privileged	N/A	A-ORA-SCHE-031120/488

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker having Local Logon privilege with logon to the infrastructure where Scheduler executes to compromise Scheduler. While the vulnerability is in Scheduler, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Scheduler. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2020-14735**		
database_vault					
N/A	21-Oct-20	6.5	Vulnerability in the Database Vault component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2 and 12.2.0.1. Easily exploitable vulnerability allows high privileged attacker having Create Public Synonym privilege with network access via Oracle Net to compromise Database Vault. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Database Vault accessible data as well as unauthorized read access to a subset of Database Vault accessible data. CVSS 3.1 Base	N/A	A-ORA-DATA-031120/489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Score 3.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2020-14736**		
sql_developer					
N/A	21-Oct-20	1.9	Vulnerability in the SQL Developer Install component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1 and 18c. Easily exploitable vulnerability allows low privileged attacker having Client Computer User Account privilege with logon to the infrastructure where SQL Developer Install executes to compromise SQL Developer Install. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of SQL Developer Install accessible data. CVSS 3.1 Base Score 2.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N). **CVE ID : CVE-2020-14740**	N/A	A-ORA-SQL_-031120/490
database_filesystem					
N/A	21-Oct-20	6.8	Vulnerability in the Database Filesystem component of Oracle Database Server.	N/A	A-ORA-DATA-031120/491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Supported versions that are affected are 11.2.0.4, 12.1.0.2 and 12.2.0.1. Easily exploitable vulnerability allows high privileged attacker having Resource, Create Table, Create View, Create Procedure, Dbfs_role privilege with network access via Oracle Net to compromise Database Filesystem. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Database Filesystem. 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-2020-14741**		
core_rdbms					
N/A	21-Oct-20	5.5	Vulnerability in the Core RDBMS 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. Easily exploitable vulnerability allows high privileged attacker having SYSDBA level account privilege with network access via Oracle Net to compromise Core RDBMS. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of	N/A	A-ORA-CORE-031120/492

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Core RDBMS 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-2020-14742**		
java_virtual_machine					
N/A	21-Oct-20	4.9	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 Procedure privilege with network access via multiple protocols to compromise Java VM. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java VM accessible data. CVSS 3.1 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2020-14743**	N/A	A-ORA-JAVA-031120/493
rest_data_services					
N/A	21-Oct-20	4	Vulnerability in the Oracle REST Data Services product of Oracle REST Data Services (component: General). Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c; Standalone ORDS: prior to	N/A	A-ORA-REST-031120/494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.2.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle REST Data Services. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle REST Data Services accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2020-14744**		
N/A	21-Oct-20	4	Vulnerability in the Oracle REST Data Services product of Oracle REST Data Services (component: General). Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c; Standalone ORDS: prior to 20.2.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle REST Data Services. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle REST Data Services 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).	N/A	A-ORA-REST-031120/495

CVSS Scoring Scale	0-1	1-2	2-3	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-2020-14745		
hyperion_lifecycle_management					
N/A	21-Oct-20	4.9	Vulnerability in the Hyperion Lifecycle Management product of Oracle Hyperion (component: Shared Services). 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 Lifecycle 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 Lifecycle 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-2020-14752**	N/A	A-ORA-HYPE-031120/496
N/A	21-Oct-20	2.1	Vulnerability in the Hyperion Lifecycle Management product of Oracle Hyperion (component: Shared Services). 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	N/A	A-ORA-HYPE-031120/497

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			compromise Hyperion Lifecycle 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 Lifecycle 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-2020-14772**		
hyperion_analytic_provider_services					
N/A	21-Oct-20	4	Vulnerability in the Hyperion Analytic Provider Services product of Oracle Hyperion (component: Smart View Provider). The supported version that is affected is 11.1.2.4. Difficult to exploit vulnerability allows low privileged attacker with access to the physical communication segment attached to the hardware where the Hyperion Analytic Provider Services executes to compromise Hyperion Analytic Provider Services. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in	N/A	A-ORA-HYPE-031120/498

CVSS Scoring Scale	0-1	1-2	2-3	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 Hyperion Analytic Provider Services accessible data as well as unauthorized read access to a subset of Hyperion Analytic Provider Services accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Hyperion Analytic Provider Services. CVSS 3.1 Base Score 4.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:L). **CVE ID : CVE-2020-14768**		
peoplesoft_enterprise_human_capital_management_global_payroll_core					
N/A	21-Oct-20	6.5	Vulnerability in the PeopleSoft Enterprise HCM Global Payroll Core product of Oracle PeopleSoft (component: Security). 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 HCM Global Payroll Core. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise HCM Global Payroll Core accessible data as well as unauthorized	N/A	A-ORA-PEOP-031120/499

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			read access to a subset of PeopleSoft Enterprise HCM Global Payroll Core accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of PeopleSoft Enterprise HCM Global Payroll Core. 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-2020-14778**		
e-business_suite_secure_enterprise_search					
N/A	21-Oct-20	6.4	Vulnerability in the Oracle E-Business Suite Secure Enterprise Search product of Oracle E-Business Suite (component: Search Integration Engine). Supported versions that are affected are 12.1.3 and 12.2.3 - 12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle E-Business Suite Secure Enterprise Search. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle E-Business Suite Secure Enterprise Search accessible data as well as unauthorized access to critical data or complete	N/A	A-ORA-E-BU-031120/500

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to all Oracle E-Business Suite Secure Enterprise Search 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-2020-14805**		
hospitality_suite					
N/A	21-Oct-20	5.8	Vulnerability in the Oracle Hospitality Suite8 product of Oracle Hospitality Applications (component: WebConnect). Supported versions that are affected are 8.10.2 and 8.11-8.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Suite8. 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 Hospitality Suite8 accessible data as well as unauthorized update, insert or delete access to some of Oracle Hospitality Suite8 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).	N/A	A-ORA-HOSP-031120/501

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
			CVE ID : CVE-2020-14807		
mysql_cluster					
N/A	21-Oct-20	4.9	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: NDBCluster Plugin). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Cluster. 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 MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 4.6 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:L). **CVE ID : CVE-2020-14853**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/502
hyperion_infrastructure_technology					
N/A	21-Oct-20	7.9	Vulnerability in the Hyperion Infrastructure Technology product of Oracle Hyperion (component: UI and Visualization). The supported version that is affected is 11.1.2.4. Easily exploitable	N/A	A-ORA-HYPE-031120/503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows high privileged attacker with network access via HTTP to compromise Hyperion Infrastructure Technology. 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 Infrastructure Technology accessible data as well as unauthorized access to critical data or complete access to all Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:N). **CVE ID : CVE-2020-14854**		
hospitality_opera_5_property_services					
N/A	21-Oct-20	8.5	Vulnerability in the Oracle Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Logging). Supported versions that are affected are 5.5 and 5.6. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Hospitality OPERA 5 Property	N/A	A-ORA-HOSP-031120/504

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Services. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 6.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2020-14858**		
N/A	21-Oct-20	7.5	Vulnerability in the Oracle Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Logging). Supported versions that are affected are 5.5 and 5.6. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hospitality OPERA 5 Property Services accessible data as well as unauthorized access to critical data or complete access to all Oracle Hospitality OPERA 5 Property Services accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity	N/A	A-ORA-HOSP-031120/505

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/ UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2020-14877**		
retail_customer_management_and_segmentation_foundation					
N/A	21-Oct-20	3.5	Vulnerability in the Oracle Retail Customer Management and Segmentation Foundation product of Oracle Retail Applications (component: Segment). Supported versions that are affected are 18.0 and 19.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Retail Customer Management and Segmentation Foundation. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Retail Customer Management and Segmentation Foundation accessible data. CVSS 3.1 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/ UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2020-14731**	N/A	A-ORA-RETA-031120/506
N/A	21-Oct-20	3.5	Vulnerability in the Oracle Retail Customer Management and Segmentation Foundation product of Oracle Retail Applications (component: Promotions). The supported version that is affected is 19.0. Difficult to	N/A	A-ORA-RETA-031120/507

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Retail Customer Management and Segmentation Foundation. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Retail Customer Management and Segmentation Foundation accessible data. CVSS 3.1 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/ UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2020-14732**		
banking_payments					
N/A	21-Oct-20	6.8	Vulnerability in the Oracle Banking Payments product of Oracle Financial Services Applications (component: Core). Supported versions that are affected are 14.1.0-14.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Payments. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Banking Payments accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/	N/A	A-ORA-BANK-031120/508

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2020-14896**		
banking_corporate_lending					
N/A	21-Oct-20	6.8	Vulnerability in the Oracle Banking Corporate Lending product of Oracle Financial Services Applications (component: Core). Supported versions that are affected are 12.3.0 and 14.0.0-14.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Corporate Lending. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Banking Corporate Lending accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2020-14894**	N/A	A-ORA-BANK-031120/509
mysql					
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/510

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2020-14672**		
N/A	21-Oct-20	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 5.7.31 and prior and 8.0.21 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-2020-14789**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/511
N/A	21-Oct-20	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server:	https://security.netapp.com/advisory	A-ORA-MYSQ-031120/512

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PS). Supported versions that are affected are 5.7.31 and prior and 8.0.21 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-2020-14790**	/ntap-20201023-0003/	
N/A	21-Oct-20	3.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.21 and prior. Difficult to exploit 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 partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.2 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/513

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2020-14791**		
N/A	21-Oct-20	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 8.0.21 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-2020-14793**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/514
N/A	21-Oct-20	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/515

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2020-14794**		
N/A	21-Oct-20	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). 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-2020-14799**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/516
N/A	21-Oct-20	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows low	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/517

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2020-14800**		
N/A	21-Oct-20	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 8.0.21 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-2020-14804**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/518
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server:	https://security.netapp.com/advisory	A-ORA-MYSQ-031120/519

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Optimizer). Supported versions that are affected are 8.0.21 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-2020-14809**	/ntap-20201023-0003/	
N/A	21-Oct-20	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Roles). Supported versions that are affected are 8.0.21 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/	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/520

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2020-14860**		
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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-2020-14861**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/521
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/522

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2020-14866**		
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 8.0.21 and prior. Difficult to exploit 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 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14867**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/523
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/524

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2020-14868**		
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: LDAP Auth). Supported versions that are affected are 5.7.31 and prior and 8.0.21 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-2020-14869**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/525
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle	https://security.netapp.c	A-ORA-MYSQ-031120/526

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MySQL (component: Server: X Plugin). Supported versions that are affected are 8.0.21 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-2020-14870**	om/advisory/ntap-20201023-0003/	
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Logging). Supported versions that are affected are 8.0.21 and prior. Difficult to exploit 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 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/527

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14873**		
N/A	21-Oct-20	7.7	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: LDAP Auth). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.1 Base Score 8.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2020-14878**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/528
N/A	21-Oct-20	7.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.31 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	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/529

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2020-14760**		
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 8.0.21 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-2020-14765**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/530
N/A	21-Oct-20	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server:	https://security.netapp.com/advisory	A-ORA-MYSQ-031120/531

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Optimizer). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 8.0.21 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-2020-14769**	/ntap-20201023-0003/	
N/A	21-Oct-20	3.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: LDAP Auth). Supported versions that are affected are 5.7.31 and prior and 8.0.21 and prior. Difficult to exploit 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 partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.2 (Availability impacts). CVSS Vector:	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/532

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2020-14771**		
N/A	21-Oct-20	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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-2020-14773**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/533
N/A	21-Oct-20	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.31 and prior and 8.0.21 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	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/534

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2020-14775**		
N/A	21-Oct-20	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.31 and prior and 8.0.21 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-2020-14776**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/535
N/A	21-Oct-20	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/536

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2020-14777**		
N/A	21-Oct-20	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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-2020-14785**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/537
N/A	21-Oct-20	4	Vulnerability in the MySQL Server product of Oracle	https://security.netapp.c	A-ORA-MYSQ-031120/538

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MySQL (component: Server: PS). Supported versions that are affected are 8.0.21 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-2020-14786**	om/advisory/ntap-20201023-0003/	
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Locking). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 8.0.21 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:	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/539

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14812**		
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.21 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-2020-14814**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/540
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.21 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	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/541

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(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-2020-14821**		
N/A	21-Oct-20	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: LDAP Auth). Supported versions that are affected are 5.7.31 and prior and 8.0.21 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 access to critical data or complete access to all MySQL Server accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2020-14827**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/542
N/A	21-Oct-20	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/543

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2020-14828**		
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.21 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-2020-14829**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/544
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows low privileged	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/545

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2020-14830**		
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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-2020-14836**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/546
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle	https://security.netapp.c	A-ORA-MYSQ-031120/547

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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-2020-14837**	om/advisory/ntap-20201023-0003/	
N/A	21-Oct-20	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.21 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 impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/548

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2020-14838**		
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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-2020-14839**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/549
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 8.0.21 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	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/550

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(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-2020-14844**		
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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-2020-14845**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/551
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/552

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2020-14846**		
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.21 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-2020-14848**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/553
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Charsets). Supported versions that are affected are	https://security.netapp.com/advisory/ntap-20201023-	A-ORA-MYSQ-031120/554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			8.0.21 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-2020-14852**	0003/	
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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-20201023-0003/	A-ORA-MYSQ-031120/555

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14888		
N/A	21-Oct-20	6.8	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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-2020-14891**	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/556
N/A	21-Oct-20	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 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	https://security.netapp.com/advisory/ntap-20201023-0003/	A-ORA-MYSQ-031120/557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2020-14893**		
jdk					
N/A	21-Oct-20	5.8	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Java SE: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. 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. 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	https://security.netapp.com/advisory/ntap-20201023-0004/	A-ORA-JDK-031120/558

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 4.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N). **CVE ID : CVE-2020-14792**		
N/A	21-Oct-20	2.6	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. 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. Successful attacks of this vulnerability can result in unauthorized read access to a subset of 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)	https://security.netapp.com/advisory/ntap-20201023-0004/	A-ORA-JDK-031120/559

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
			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 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N). **CVE ID : CVE-2020-14796**		
N/A	21-Oct-20	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: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. 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. 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	https://security.netapp.com/advisory/ntap-20201023-0004/	A-ORA-JDK-031120/560

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2020-14797**		
N/A	21-Oct-20	2.6	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. 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. 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 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-20201023-0004/	A-ORA-JDK-031120/561

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
			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 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N). **CVE ID : CVE-2020-14798**		
N/A	21-Oct-20	5	Vulnerability in the Java SE product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 11.0.8 and 15. 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 read access to a subset of Java SE 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	https://security.netapp.com/advisory/ntap-20201023-0004/	A-ORA-JDK-031120/562

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
			administrator). 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-2020-14803**		
N/A	21-Oct-20	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported versions that are affected are Java SE: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. 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:	https://security.netapp.com/advisory/ntap-20201023-0004/	A-ORA-JDK-031120/563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2020-14779**		
N/A	21-Oct-20	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JNDI). Supported versions that are affected are Java SE: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. 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-2020-14781**	https://security.netapp.com/advisory/ntap-20201023-0004/	A-ORA-JDK-031120/564

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	21-Oct-20	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: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. 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. 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-2020-14782**	https://security.netapp.com/advisory/ntap-20201023-0004/	A-ORA-JDK-031120/565
jre					
N/A	21-Oct-20	5.8	Vulnerability in the Java SE,	https://secu	A-ORA-JRE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Java SE Embedded product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Java SE: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. 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. 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 4.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/	rity.netapp.com/advisory/ntap-20201023-0004/	031120/566

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
			UI:R/S:U/C:L/I:L/A:N). **CVE ID : CVE-2020-14792**		
N/A	21-Oct-20	2.6	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. 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. Successful attacks of this vulnerability can result in unauthorized read access to a subset of 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 3.1 (Confidentiality impacts). CVSS Vector:	https://security.netapp.com/advisory/ntap-20201023-0004/	A-ORA-JRE-031120/567

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N). **CVE ID : CVE-2020-14796**		
N/A	21-Oct-20	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: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. 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. 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).	https://security.netapp.com/advisory/ntap-20201023-0004/	A-ORA-JRE-031120/568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14797		
N/A	21-Oct-20	2.6	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. 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. 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 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 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/	https://security.netapp.com/advisory/ntap-20201023-0004/	A-ORA-JRE-031120/569

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UI:R/S:U/C:N/I:L/A:N). **CVE ID : CVE-2020-14798**		
N/A	21-Oct-20	5	Vulnerability in the Java SE product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 11.0.8 and 15. 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 read access to a subset of Java SE 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 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-2020-14803**	https://security.netapp.com/advisory/ntap-20201023-0004/	A-ORA-JRE-031120/570
N/A	21-Oct-20	4.3	Vulnerability in the Java SE, Java SE Embedded product of	https://security.netapp.c	A-ORA-JRE-031120/571

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle Java SE (component: Serialization). Supported versions that are affected are Java SE: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. 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-2020-14779**	om/advisory/ntap-20201023-0004/	
N/A	21-Oct-20	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JNDI). Supported versions that are affected are Java SE:	https://security.netapp.com/advisory/ntap-20201023-	A-ORA-JRE-031120/572

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. 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-2020-14781**	0004/	
N/A	21-Oct-20	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: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. Difficult to exploit vulnerability allows	https://security.netapp.com/advisory/ntap-20201023-0004/	A-ORA-JRE-031120/573

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 update, insert or delete access to some 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 (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-2020-14782**		
vm_virtualbox					
N/A	21-Oct-20	7.2	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.16. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure	N/A	A-ORA-VM_V-031120/574

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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-2020-14872**		
N/A	21-Oct-20	4.9	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.16. 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-031120/575

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(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-2020-14881**		
N/A	21-Oct-20	4.9	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.16. 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 (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-2020-14884**	N/A	A-ORA-VM_V-031120/576
N/A	21-Oct-20	4.9	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.16.	N/A	A-ORA-VM_V-031120/577

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 (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-2020-14885**		
N/A	21-Oct-20	4.9	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.16. 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	N/A	A-ORA-VM_V-031120/578

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 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-2020-14886**		
N/A	21-Oct-20	4.9	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.16. 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 (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-2020-14889**	N/A	A-ORA-VM_V-031120/579

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	21-Oct-20	4.9	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.16. Easily exploitable vulnerability allows low 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 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14892**	N/A	A-ORA-VM_V-031120/580
flexcube_direct_banking					
N/A	21-Oct-20	7.1	Vulnerability in the Oracle FLEXCUBE Direct Banking product of Oracle Financial Services Applications (component: Pre Login). Supported versions that are affected are 12.0.1, 12.0.2 and 12.0.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle FLEXCUBE Direct Banking. Successful attacks require	N/A	A-ORA-FLEX-031120/581

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 FLEXCUBE Direct Banking accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N). **CVE ID : CVE-2020-14890**		
N/A	21-Oct-20	7.1	Vulnerability in the Oracle FLEXCUBE Direct Banking product of Oracle Financial Services Applications (component: Pre Login). Supported versions that are affected are 12.0.1, 12.0.2 and 12.0.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle FLEXCUBE Direct Banking. 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 FLEXCUBE Direct Banking accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/	N/A	A-ORA-FLEX-031120/582

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UI:R/S:U/C:H/I:N/A:N). **CVE ID : CVE-2020-14897**		
business_intelligence_publisher					
N/A	21-Oct-20	7.5	Vulnerability in the BI Publisher product of Oracle Fusion Middleware (component: E-Business Suite - XDO). 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 low privileged attacker with network access via HTTP to compromise BI Publisher. While the vulnerability is in 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 BI Publisher accessible data as well as unauthorized update, insert or delete access to some of BI Publisher accessible data. CVSS 3.1 Base Score 8.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N). **CVE ID : CVE-2020-14879**	N/A	A-ORA-BUSI-031120/583
N/A	21-Oct-20	7.5	Vulnerability in the BI Publisher product of Oracle Fusion Middleware (component: E-Business Suite - XDO). Supported versions that are affected are 5.5.0.0.0,	N/A	A-ORA-BUSI-031120/584

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 BI Publisher. While the vulnerability is in 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 BI Publisher accessible data as well as unauthorized update, insert or delete access to some of BI Publisher accessible data. CVSS 3.1 Base Score 8.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N). **CVE ID : CVE-2020-14880**		
N/A	21-Oct-20	5.8	Vulnerability in the BI Publisher product of Oracle Fusion Middleware (component: BI Publisher Security). 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 BI Publisher. Successful attacks require human interaction from a person other than the attacker. Successful attacks of	N/A	A-ORA-BUSI-031120/585

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability can result in unauthorized access to critical data or complete access to all BI Publisher accessible data as well as unauthorized update, insert or delete access to some of 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-2020-14780**		
N/A	21-Oct-20	5.8	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 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,	N/A	A-ORA-BUSI-031120/586

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2020-14784**		
N/A	21-Oct-20	5.8	Vulnerability in the BI Publisher product of Oracle Fusion Middleware (component: BI Publisher Security). 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 BI Publisher. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in 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 BI Publisher accessible data as well as unauthorized update, insert or delete access to some of BI Publisher accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector:	N/A	A-ORA-BUSI-031120/587

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-2020-14842**		
one-to-one_fulfillment					
N/A	21-Oct-20	7.8	Vulnerability in the Oracle One-to-One Fulfillment product of Oracle E-Business Suite (component: Print Server). 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 One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, 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 One-to-One Fulfillment accessible data as well as unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment 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-2020-14863**	N/A	A-ORA-ONE--031120/588

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	21-Oct-20	5.8	Vulnerability in the Oracle One-to-One Fulfillment product of Oracle E-Business Suite (component: Print Server). The supported version that is affected is 12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, 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 One-to-One Fulfillment accessible data as well as unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment 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-2020-14819**	N/A	A-ORA-ONE--031120/589
marketing					
N/A	21-Oct-20	9.4	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component:	N/A	A-ORA-MARK-031120/590

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Marketing Administration). Supported versions that are affected are 12.1.1 - 12.1.3 and 12.2.3 - 12.2.10. 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 (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-2020-14875**		
N/A	21-Oct-20	5.8	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 - 12.2.10. 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 vulnerability is in	N/A	A-ORA-MARK-031120/591

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle Marketing, 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 Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing 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-2020-14816**		
N/A	21-Oct-20	5.8	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 - 12.2.10. 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 vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete	N/A	A-ORA-MARK-031120/592

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to all Oracle Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing 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-2020-14817**		
N/A	21-Oct-20	5.8	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 - 12.2.10. 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 vulnerability is in Oracle Marketing, 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 Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity	N/A	A-ORA-MARK-031120/593

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2020-14831**		
N/A	21-Oct-20	5.8	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. 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 vulnerability is in Oracle Marketing, 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 Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing 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-2020-14835**	N/A	A-ORA-MARK-031120/594
N/A	21-Oct-20	5.8	Vulnerability in the Oracle Marketing product of Oracle	N/A	A-ORA-MARK-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			E-Business Suite (component: Marketing Administration). Supported versions that are affected are 12.1.1 - 12.1.3 and 12.2.3 - 12.2.10. 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 vulnerability is in Oracle Marketing, 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 Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing 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-2020-14849**		031120/595
business_intelligence					
N/A	21-Oct-20	7.8	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Installation). Supported versions that are affected are 5.5.0.0.0,	N/A	A-ORA-BUSI-031120/596

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. 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-2020-14864**		
N/A	21-Oct-20	5.5	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Web Administration). 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 low privileged 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	N/A	A-ORA-BUSI-031120/597

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			data as well as unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition 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-2020-14766**		
N/A	21-Oct-20	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, 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	N/A	A-ORA-BUSI-031120/598

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			well as unauthorized update, insert or delete access to some of Oracle Business 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-2020-14815**		
N/A	21-Oct-20	6.8	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, 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 update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized	N/A	A-ORA-BUSI-031120/599

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Business Intelligence Enterprise Edition. CVSS 3.1 Base Score 7.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L). **CVE ID : CVE-2020-14843**		
application_object_library					
N/A	21-Oct-20	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 - 12.2.10. 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	N/A	A-ORA-APPL-031120/600

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2020-14840**		
trade_management					
N/A	21-Oct-20	5.8	Vulnerability in the Oracle Trade Management product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.1.3 and 12.2.3 - 12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, 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 Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management accessible data. CVSS 3.1 Base	N/A	A-ORA-TRAD-031120/601

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2020-14808**		
N/A	21-Oct-20	8.5	Vulnerability in the Oracle Trade Management product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.1.1 - 12.1.3 and 12.2.3 - 12.2.10. 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-2020-14876**	N/A	A-ORA-TRAD-031120/602
N/A	21-Oct-20	5.8	Vulnerability in the Oracle Trade Management product of Oracle E-Business Suite (component: User Interface). Supported versions that are	N/A	A-ORA-TRAD-031120/603

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected are 12.1.1 - 12.1.3 and 12.2.3 - 12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, 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 Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management 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-2020-14833**		
N/A	21-Oct-20	5.8	Vulnerability in the Oracle Trade Management product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.1.1 - 12.1.3 and 12.2.3 - 12.2.10. Easily exploitable vulnerability allows unauthenticated	N/A	A-ORA-TRAD-031120/604

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, 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 Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management 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-2020-14834**		
N/A	21-Oct-20	7.8	Vulnerability in the Oracle Trade Management product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.1.1 - 12.1.3 and 12.2.3 - 12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require	N/A	A-ORA-TRAD-031120/605

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 Trade Management, 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 Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management 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-2020-14851**		
N/A	21-Oct-20	7.8	Vulnerability in the Oracle Trade Management product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.1.1 - 12.1.3 and 12.2.3 - 12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle	N/A	A-ORA-TRAD-031120/606

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Trade Management, 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 Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management 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-2020-14856**		
N/A	21-Oct-20	5.8	Vulnerability in the Oracle Trade Management product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.1.1 - 12.1.3 and 12.2.3 - 12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, attacks may significantly impact additional products. Successful attacks of this	N/A	A-ORA-TRAD-031120/607

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 Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management 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-2020-14857**		
applications_framework					
N/A	21-Oct-20	5.8	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Popup windows). Supported versions that are affected are 12.1.3 and 12.2.3 - 12.2.10. 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	N/A	A-ORA-APPL-031120/608

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized update, insert or delete access to some of Oracle Applications Framework 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-2020-14746**		
hyperion_bi\+					
N/A	21-Oct-20	2.1	Vulnerability in the Hyperion BI+ product of Oracle Hyperion (component: IQR-Foundation service). The supported version that is affected is 11.1.2.4. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise 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 Hyperion BI+ accessible 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-2020-14767**	N/A	A-ORA-HYPE-031120/609
N/A	21-Oct-20	2.1	Vulnerability in the Hyperion BI+ product of Oracle Hyperion (component: IQR-Foundation service). The	N/A	A-ORA-HYPE-031120/610

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			supported version that is affected is 11.1.2.4. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise Hyperion BI+. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Hyperion BI+ accessible data. CVSS 3.1 Base Score 2.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:N). **CVE ID : CVE-2020-14770**		
flexcube_universal_banking					
N/A	21-Oct-20	6.8	Vulnerability in the Oracle FLEXCUBE Universal Banking product of Oracle Financial Services Applications (component: Infrastructure). Supported versions that are affected are 12.3.0 and 14.0.0-14.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle FLEXCUBE Universal Banking	N/A	A-ORA-FLEX-031120/611

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2020-14887**		
hyperion_planning					
N/A	21-Oct-20	2.1	Vulnerability in the Hyperion Planning product of Oracle Hyperion (component: Application Development Framework). 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 Planning. 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 Planning 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-2020-14764**	N/A	A-ORA-HYPE-031120/612
hospitality_suite8					
N/A	21-Oct-20	5.8	Vulnerability in the Oracle Hospitality Suite8 product of Oracle Hospitality Applications (component: WebConnect). Supported	N/A	A-ORA-HOSP-031120/613

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions that are affected are 8.10.2 and 8.11-8.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Suite8. 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 Hospitality Suite8 accessible data as well as unauthorized read access to a subset of Oracle Hospitality Suite8 accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N). **CVE ID : CVE-2020-14810**		
graalvm					
N/A	21-Oct-20	5	Vulnerability in the Java SE product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 11.0.8 and 15. 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 read access to a	https://security.netapp.com/advisory/ntap-20201023-0004/	A-ORA-GRAA-031120/614

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			subset of Java SE 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 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-2020-14803**		
financial_services_analytical_applications_infrastructure					
N/A	21-Oct-20	7.8	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. While the vulnerability is in Oracle Financial Services Analytical	N/A	A-ORA-FINA-031120/615

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Applications Infrastructure, 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 Financial Services Analytical Applications Infrastructure. CVSS 3.1 Base Score 8.6 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H). **CVE ID : CVE-2020-14824**		
applications_manager					
N/A	21-Oct-20	6.4	Vulnerability in the Oracle Applications Manager product of Oracle E-Business Suite (component: Oracle Diagnostics Interfaces). Supported versions that are affected are 12.1.3 and 12.2.3 - 12.2.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Manager. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Applications Manager accessible data as well as unauthorized read access to a subset of Oracle Applications Manager accessible data.	N/A	A-ORA-APPL-031120/616

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2020-14761**		
N/A	21-Oct-20	5	Vulnerability in the Oracle Applications Manager product of Oracle E-Business Suite (component: AMP EBS Integration). Supported versions that are affected are 12.1.3 and 12.2.3 - 12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Manager. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Applications Manager 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-2020-14811**	N/A	A-ORA-APPL-031120/617
N/A	21-Oct-20	5	Vulnerability in the Oracle Applications Manager product of Oracle E-Business Suite (component: SQL Extensions). Supported versions that are affected are 12.1.3 and 12.2.3 - 12.2.10. Easily exploitable vulnerability allows unauthenticated attacker	N/A	A-ORA-APPL-031120/618

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with network access via HTTP to compromise Oracle Applications Manager. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Applications Manager 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-2020-14826**		
installed_base					
N/A	21-Oct-20	4.3	Vulnerability in the Oracle Installed Base product of Oracle E-Business Suite (component: APIs). Supported versions that are affected are 12.1.1 - 12.1.3 and 12.2.3 - 12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Installed Base. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Installed Base, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Installed Base	N/A	A-ORA-INST-031120/619

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2020-14822**		
weblogic_server					
N/A	21-Oct-20	10	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 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-2020-14859**	N/A	A-ORA-WEBL-031120/620
N/A	21-Oct-20	10	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, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable	N/A	A-ORA-WEBL-031120/621

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 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-2020-14882**		
N/A	21-Oct-20	6.8	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). The supported version that is affected is 12.2.1.3.0. 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	N/A	A-ORA-WEBL-031120/622

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(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-2020-14757**		
N/A	21-Oct-20	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, 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-2020-14820**	N/A	A-ORA-WEBL-031120/623
N/A	21-Oct-20	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	N/A	A-ORA-WEBL-031120/624

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2020-14825**		
N/A	21-Oct-20	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, 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 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-2020-14841**	N/A	A-ORA-WEBL-031120/625
N/A	21-Oct-20	9	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware	N/A	A-ORA-WEBL-031120/626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(component: Console). 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 takeover of Oracle WebLogic 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-2020-14883**		
hospitality_reporting_and_analytics					
N/A	21-Oct-20	1.9	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 and	N/A	A-ORA-HOSP-031120/627

CVSS Scoring Scale	0-1	1-2	2-3	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 Hospitality Reporting and Analytics, 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 Hospitality Reporting and Analytics accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:N/A:N). **CVE ID : CVE-2020-14753**		
communications_diameter_signaling_router					
N/A	21-Oct-20	5.8	Vulnerability in the Oracle Communications Diameter Signaling Router (DSR) product of Oracle Communications (component: User Interface). Supported versions that are affected are 8.0.0.0-8.4.0.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Communications Diameter Signaling Router (DSR). Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Communications Diameter	N/A	A-ORA-COMM-031120/628

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Signaling Router (DSR), attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Communications Diameter Signaling Router (DSR) accessible data as well as unauthorized read access to a subset of Oracle Communications Diameter Signaling Router (DSR) 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-2020-14788**		
N/A	21-Oct-20	4.9	Vulnerability in the Oracle Communications Diameter Signaling Router (DSR) product of Oracle Communications (component: User Interface). Supported versions that are affected are 8.0.0.0-8.4.0.5. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Communications Diameter Signaling Router (DSR). Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle	N/A	A-ORA-COMM-031120/629

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
			Communications Diameter Signaling Router (DSR), attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Communications Diameter Signaling Router (DSR) accessible data as well as unauthorized read access to a subset of Oracle Communications Diameter Signaling Router (DSR) 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-2020-14787**		
peoplesoft_enterprise_peopletools					
N/A	21-Oct-20	4.3	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: PIA Core Technology). Supported versions that are affected are 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.	N/A	A-ORA-PEOP-031120/630

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N). **CVE ID : CVE-2020-14795**		
N/A	21-Oct-20	4.3	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: PIA Core Technology). 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 Enterprise PeopleTools accessible data as well as unauthorized read	N/A	A-ORA-PEOP-031120/631

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2020-14801**		
N/A	21-Oct-20	4.3	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: PIA Core Technology). 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 Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data.	N/A	A-ORA-PEOP-031120/632

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
			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-2020-14802**		
N/A	21-Oct-20	5	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 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-2020-14806**	N/A	A-ORA-PEOP-031120/633
N/A	21-Oct-20	5.8	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: PIA Grids). Supported versions that are affected are 8.56, 8.57 and 8.58. Easily exploitable vulnerability allows	N/A	A-ORA-PEOP-031120/634

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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-2020-14813**		
N/A	21-Oct-20	5.8	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Integration Broker). 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	N/A	A-ORA-PEOP-031120/635

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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-2020-14832**		
N/A	21-Oct-20	4	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 high privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in	N/A	A-ORA-PEOP-031120/636

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools 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-2020-14847**		
database					
N/A	21-Oct-20	6.8	Vulnerability in the RDBMS Security component of Oracle Database Server. The supported version that is affected is 19c. Easily exploitable vulnerability allows high privileged attacker having Analyze Any privilege with network access via Oracle Net to compromise RDBMS Security. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all RDBMS Security 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-2020-14901**	N/A	A-ORA-DATA-031120/637
orchid					
platform					
Improper Neutralization of Input During Web Page	19-Oct-20	4.3	In platform before version 9.4.4, inline attributes are not properly escaped. If the data that came from users was not escaped, then an XSS	https://github.com/orchidsoftware/platform/security/advisorie	A-ORC-PLAT-031120/638

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			vulnerability is possible. The issue was introduced in 9.0.0 and fixed in 9.4.4. **CVE ID : CVE-2020-15263**	s/GHSA-589w-hccm-265x	
Oscommerce					
oscommerce					
Cross-Site Request Forgery (CSRF)	28-Oct-20	6.8	osCommerce Phoenix CE before 1.0.5.4 allows admin/define_language.php CSRF. **CVE ID : CVE-2020-27975**	N/A	A-OSC-OSCO-031120/639
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Oct-20	10	osCommerce Phoenix CE before 1.0.5.4 allows OS command injection remotely. Within admin/mail.php, a from POST parameter can be passed to the application. This affects the PHP mail function, and the sendmail -f option. **CVE ID : CVE-2020-27976**	N/A	A-OSC-OSCO-031120/640
osm-static-maps_project					
osm-static-maps					
Server-Side Request Forgery (SSRF)	20-Oct-20	6.5	This affects all versions of package osm-static-maps. User input given to the package is passed directly to a template without escaping ({{{ ... }}}). As such, it is possible for an attacker to inject arbitrary HTML/JS code and depending on the context. It will be outputted as an HTML on the page which gives opportunity for XSS or rendered on the server (puppeteer) which also gives opportunity for SSRF and	N/A	A-OSM-OSM--031120/641

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Local File Read. **CVE ID : CVE-2020-7749**		
overwolf					
overwolf					
N/A	16-Oct-20	9.3	In the client in Overwolf 0.149.2.30, a channel can be accessed or influenced by an actor that is not an endpoint. **CVE ID : CVE-2020-25214**	N/A	A-OVE-OVER-031120/642
parseplatform					
parse-server					
Operation on a Resource after Expiration or Release	22-Oct-20	4	Parse Server (npm package parse-server) broadcasts events to all clients without checking if the session token is valid. This allows clients with expired sessions to still receive subscription objects. It is not possible to create subscription objects with invalid session tokens. The issue is not patched. **CVE ID : CVE-2020-15270**	https://github.com/parse-community/parse-server/security/advisories/GHSA-2xm2-xj2q-qgpj	A-PAR-PARS-031120/643
phpredisadmin_project					
phpredisadmin					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-20	4.3	phpRedisAdmin before 1.13.2 allows XSS via the login.php username parameter. **CVE ID : CVE-2020-27163**	N/A	A-PHP-PHPR-031120/644
Powerdns					
recursor					
N/A	16-Oct-20	5	An issue has been found in	https://docs.	A-POW-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PowerDNS Recursor before 4.1.18, 4.2.x before 4.2.5, and 4.3.x before 4.3.5. A remote attacker can cause the cached records for a given name to be updated to the Bogus DNSSEC validation state, instead of their actual DNSSEC Secure state, via a DNS ANY query. This results in a denial of service for installation that always validate (dnssec=validate), and for clients requesting validation when on-demand validation is enabled (dnssec=process). **CVE ID : CVE-2020-25829**	powerdns.com/recursor/security-advisories/powerdns-advisory-2020-07.html	RECU-031120/645
Pulsesecure					
pulse_secure_desktop					
Weak Password Requirements	27-Oct-20	1.9	Pulse Secure Desktop Client 9.0Rx before 9.0R5 and 9.1Rx before 9.1R4 on Windows reveals users' passwords if Save Settings is enabled. **CVE ID : CVE-2020-8956**	N/A	A-PUL-PULS-031120/646
pulse_secure_desktop_client					
Improper Privilege Management	28-Oct-20	4.6	A vulnerability in the Pulse Secure Desktop Client (Linux) < 9.1R9 could allow local attackers to escalate privilege. **CVE ID : CVE-2020-8248**	N/A	A-PUL-PULS-031120/647
Improper Privilege Management	28-Oct-20	4.6	A vulnerability in the Pulse Secure Desktop Client (Linux) < 9.1R9 could allow local attackers to escalate privilege.	N/A	A-PUL-PULS-031120/648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8250		
N/A	28-Oct-20	4	A vulnerability in the Pulse Connect Secure < 9.1R9 admin web interface could allow an authenticated attacker to perform an arbitrary file reading vulnerability is fixed using encrypted URL blacklisting that prevents these messages. **CVE ID : CVE-2020-8255**	N/A	A-PUL-PULS-031120/649
Unrestricted Upload of File with Dangerous Type	28-Oct-20	6.5	A vulnerability in the Pulse Connect Secure < 9.1R9 admin web interface could allow an authenticated attacker to perform an arbitrary code execution using uncontrolled gzip extraction. **CVE ID : CVE-2020-8260**	N/A	A-PUL-PULS-031120/650
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Oct-20	3.5	A vulnerability in the authenticated user web interface of Pulse Connect Secure < 9.1R9 could allow attackers to conduct Cross-Site Scripting (XSS) through the CGI file. **CVE ID : CVE-2020-8263**	N/A	A-PUL-PULS-031120/651
Qemu					
qemu					
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Oct-20	2.1	An issue was discovered in QEMU through 5.1.0. An out-of-bounds memory access was found in the ATI VGA device implementation. This flaw occurs in the ati_2d_blt() routine in hw/display/ati_2d.c while	N/A	A-QEM-QEMU-031120/652

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			handling MMIO write operations through the ati_mm_write() callback. A malicious guest could use this flaw to crash the QEMU process on the host, resulting in a denial of service. **CVE ID : CVE-2020-24352**		
raiseitsolutions					
rits_browser					
Improper Restriction of Rendered UI Layers or Frames	20-Oct-20	4.3	User Interface (UI) Misrepresentation of Critical Information vulnerability in the address bar of the Yandex Browser allows an attacker to obfuscate the true source of data as presented in the browser. This issue affects the RITS Browser version 3.3.9 and prior versions. **CVE ID : CVE-2020-7371**	N/A	A-RAI-RITS-031120/653
rconfig					
rconfig					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Oct-20	9	rConfig 3.9.4 and earlier allows authenticated code execution (of system commands) by sending a forged GET request to lib/ajaxHandlers/ajaxAddTemplate.php or lib/ajaxHandlers/ajaxEditTemplate.php. **CVE ID : CVE-2020-13778**	N/A	A-RCO-RCON-031120/654
Redhat					
openshift_application_runtimes					
Improper Authenticati	16-Oct-20	6.3	A flaw was found in JBoss EAP, where the	N/A	A-RED-OPEN-031120/655

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			authentication configuration is set-up using a legacy SecurityRealm, to delegate to a legacy PicketBox SecurityDomain, and then reloaded to admin-only mode. This flaw allows an attacker to perform a complete authentication bypass by using an arbitrary user and password. The highest threat to vulnerability is to system availability. **CVE ID : CVE-2020-14299**		
jboss_enterprise_application_platform					
Improper Authentication	16-Oct-20	6.3	A flaw was found in JBoss EAP, where the authentication configuration is set-up using a legacy SecurityRealm, to delegate to a legacy PicketBox SecurityDomain, and then reloaded to admin-only mode. This flaw allows an attacker to perform a complete authentication bypass by using an arbitrary user and password. The highest threat to vulnerability is to system availability. **CVE ID : CVE-2020-14299**	N/A	A-RED-JBOS-031120/656
single_sign-on					
Improper Authentication	16-Oct-20	6.3	A flaw was found in JBoss EAP, where the authentication configuration is set-up using a legacy SecurityRealm, to delegate to a legacy PicketBox SecurityDomain, and then	N/A	A-RED-SING-031120/657

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reloaded to admin-only mode. This flaw allows an attacker to perform a complete authentication bypass by using an arbitrary user and password. The highest threat to vulnerability is to system availability. **CVE ID : CVE-2020-14299**		
fabric8-maven					
Deserialization of Untrusted Data	22-Oct-20	6.9	A flaw was found in the fabric8-maven-plugin 4.0.0 and later. When using a wildfly-swarm or thorntail custom configuration, a malicious YAML configuration file on the local machine executing the maven plug-in could allow for deserialization of untrusted data resulting in arbitrary code execution. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2020-10721**	N/A	A-RED-FABR-031120/658
requarks					
wiki.js					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-20	3.5	In Wiki.js before version 2.5.162, an XSS payload can be injected in a page title and executed via the search results. While the title is properly escaped in both the navigation links and the actual page title, it is not the case in the search results. Commit	https://github.com/Requarks/wiki/security/advisories/GHSA-pgjv-84m7-62q7	A-REQ-WIKI-031120/659

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a57d9af34c15adbf460dde6553d964efddf433de fixes this vulnerability (version 2.5.162) by properly escaping the text content displayed in the search results. **CVE ID : CVE-2020-15274**		
Sage					
easypay					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Oct-20	3.5	Multiple stored cross-site scripting (XSS) vulnerabilities in Sage EasyPay 10.7.5.10 allow authenticated attackers to inject arbitrary web script or HTML via multiple parameters through Unicode Transformations (Best-fit Mapping), as demonstrated by the full-width variants of the less-than sign (%EF%BC%9C) and greater-than sign (%EF%BC%9E). **CVE ID : CVE-2020-13893**	N/A	A-SAG-EASY-031120/660
sagedpw					
sage_dpw					
Unrestricted Upload of File with Dangerous Type	16-Oct-20	4.3	An issue was discovered in Sage DPW 2020_06_x before 2020_06_002. It allows unauthenticated users to upload JavaScript (in a file) via the expenses claiming functionality. However, to view the file, authentication is required. By exploiting this vulnerability, an attacker can persistently include arbitrary HTML or JavaScript code into the affected web page. The vulnerability can be used to	N/A	A-SAG-SAGE-031120/661

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			change the contents of the displayed site, redirect to other sites, or steal user credentials. Additionally, users are potential victims of browser exploits and JavaScript malware. **CVE ID : CVE-2020-26583**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-20	4.3	An issue was discovered in Sage DPW 2020_06_x before 2020_06_002. The search field "Kurs suchen" on the page Kurskatalog is vulnerable to Reflected XSS. If the attacker can lure a user into clicking a crafted link, he can execute arbitrary JavaScript code in the user's browser. The vulnerability can be used to change the contents of the displayed site, redirect to other sites, or steal user credentials. Additionally, users are potential victims of browser exploits and JavaScript malware. **CVE ID : CVE-2020-26584**	N/A	A-SAG-SAGE-031120/662
SAP					
3d_visual_enterprise_viewer					
N/A	20-Oct-20	4.3	SAP 3D Visual Enterprise Viewer, version 9, allows an attacker to send certain manipulated file to the victim, which can lead to leakage of sensitive information when the victim loads the malicious file into the VE viewer, leading to Information	N/A	A-SAP-3D_V-031120/663

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Disclosure. **CVE ID : CVE-2020-6315**		
banking_services					
Incorrect Authorization	20-Oct-20	6.8	SAP Banking Services version 500, use an incorrect authorization object in some of its reports. Although the affected reports are protected with otherauthorization objects, exploitation of the vulnerability could lead to privilege escalation and violation in segregation of duties, which in turn could lead to Service interruptions and system unavailability for the victim and users of the component. **CVE ID : CVE-2020-6362**	N/A	A-SAP-BANK-031120/664
netweaver_compare_systems					
Improper Input Validation	20-Oct-20	5.5	SAP NetWeaver (Compare Systems) versions - 7.20, 7.30, 7.40, 7.50, does not sufficiently validate uploaded XML documents. An attacker with administrative privileges can retrieve arbitrary files including files on OS level from the server and/or can execute a denial-of-service. **CVE ID : CVE-2020-6366**	N/A	A-SAP-NETW-031120/665
netweaver_composite_application_framework					
Improper Neutralization of Input During Web Page	20-Oct-20	4.3	There is a reflected cross site scripting vulnerability in SAP NetWeaver Composite Application Framework, versions - 7.20, 7.30, 7.31,	N/A	A-SAP-NETW-031120/666

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			7.40, 7.50. An unauthenticated attacker can trick an unsuspecting authenticated user to click on a malicious link. The end users browser has no way to know that the script should not be trusted, and will execute the script, resulting in sensitive information being disclosed or modified. **CVE ID : CVE-2020-6367**		
focused_run					
N/A	20-Oct-20	4.3	SAP Solution Manager and SAP Focused Run (update provided in WILY_INTRO_ENTERPRISE 9.7, 10.1, 10.5, 10.7), allows an unauthenticated attackers to bypass the authentication if the default passwords for Admin and Guest have not been changed by the administrator.This may impact the confidentiality of the service. **CVE ID : CVE-2020-6369**	N/A	A-SAP-FOCU-031120/667
netweaver_design_time_repository					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-20	3.5	SAP NetWeaver Design Time Repository (DTR), versions - 7.11, 7.30, 7.31, 7.40, 7.50, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. **CVE ID : CVE-2020-6370**	N/A	A-SAP-NETW-031120/668
solution_manager					
N/A	20-Oct-20	4.3	SAP Solution Manager and	N/A	A-SAP-SOLU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SAP Focused Run (update provided in WILY_INTRO_ENTERPRISE 9.7, 10.1, 10.5, 10.7), allows an unauthenticated attackers to bypass the authentication if the default passwords for Admin and Guest have not been changed by the administrator.This may impact the confidentiality of the service. **CVE ID : CVE-2020-6369**		031120/669
businessobjects_business_intelligence_platform					
Server-Side Request Forgery (SSRF)	20-Oct-20	5	SAP BusinessObjects Business Intelligence Platform (Web Services) versions - 410, 420, 430, allows an unauthenticated attacker to inject arbitrary values as CMS parameters to perform lookups on the internal network which is otherwise not accessible externally. On successful exploitation, attacker can scan internal network to determine internal infrastructure and gather information for further attacks like remote file inclusion, retrieve server files, bypass firewall and force the vulnerable server to perform malicious requests, resulting in a Server-Side Request Forgery vulnerability. **CVE ID : CVE-2020-6308**	N/A	A-SAP-BUSI-031120/670

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
scratch					
scratch-svg-renderer					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Oct-20	6.8	This affects the package scratch-svg-renderer before 0.2.0-prerelease.20201019174008. The loadString function does not escape SVG properly, which can be used to inject arbitrary elements into the DOM via the _transformMeasurements function. **CVE ID : CVE-2020-7750**	N/A	A-SCR-SCRA-031120/671
Snort					
snort					
N/A	21-Oct-20	5	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured File Policy for HTTP. The vulnerability is due to incorrect detection of modified HTTP packets used in chunked responses. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass a configured File Policy for HTTP packets and deliver a malicious payload. **CVE ID : CVE-2020-3299**	N/A	A-SNO-SNOR-031120/672
Solarwinds					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n-central					
Session Fixation	19-Oct-20	6.8	SolarWinds N-central through 2020.1 allows session hijacking and requires user interaction or physical access. The N-Central JSESSIONID cookie attribute is not checked against multiple sources such as sourceip, MFA claim, etc. as long as the victim stays logged in within N-Central. To take advantage of this, cookie could be stolen and the JSESSIONID can be captured. On its own this is not a surprising result; low security tools allow the cookie to roam from machine to machine. The JSESSION cookie can then be used on the attackers' workstation by browsing to the victim's NCentral server URL and replacing the JSESSIONID attribute value by the captured value. Expected behavior would be to check this against a second source and enforce at least a reauthentication or multi factor request as N-Central is a highly privileged service. **CVE ID : CVE-2020-15909**	N/A	A-SOL-N-CE-031120/673
Incorrect Permission Assignment for Critical Resource	19-Oct-20	4.3	SolarWinds N-Central version 12.3 GA and lower does not set the JSESSIONID attribute to HTTPOnly. This makes it possible to influence the cookie with javascript. An	N/A	A-SOL-N-CE-031120/674

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could send the user to a prepared webpage or by influencing JavaScript to the extract the JESSIONID. This could then be forwarded to the attacker. **CVE ID : CVE-2020-15910**		
Sonicwall					
global_vpn_client					
Uncontrolled Search Path Element	28-Oct-20	6.9	SonicWall Global VPN client version 4.10.4.0314 and earlier have an insecure library loading (DLL hijacking) vulnerability. Successful exploitation could lead to remote code execution in the target system. **CVE ID : CVE-2020-5145**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2020-0021	A-SON-GLOB-031120/675
sparksolutions					
spree					
Insufficient Session Expiration	20-Oct-20	6.4	In Spree before versions 3.7.11, 4.0.4, or 4.1.11, expired user tokens could be used to access Storefront API v2 endpoints. The issue is patched in versions 3.7.11, 4.0.4 and 4.1.11. A workaround without upgrading is described in the linked advisory. **CVE ID : CVE-2020-15269**	https://github.com/spree/spree/security/advisories/GHSA-f8cm-364f-q9qh	A-SPA-SPRE-031120/676
strapi					
strapi					
N/A	22-Oct-20	7.5	admin/src/containers/InputModalStepperProvider/index.js in Strapi before 3.2.5 has	N/A	A-STR-STRA-031120/677

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unwanted /proxy?url= functionality. **CVE ID : CVE-2020-27664**		
Incorrect Default Permissions	22-Oct-20	5	In Strapi before 3.2.5, there is no admin::hasPermissions restriction for CTB (aka content-type-builder) routes. **CVE ID : CVE-2020-27665**	N/A	A-STR-STRA-031120/678
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Oct-20	3.5	Strapi before 3.2.5 has stored XSS in the wysiwyg editor's preview feature. **CVE ID : CVE-2020-27666**	N/A	A-STR-STRA-031120/679
sylius					
sylius					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Oct-20	3.5	In Sylius before versions 1.6.9, 1.7.9 and 1.8.3, the user may register in a shop by email mail@example.com, verify it, change it to the mail another@domain.com and stay verified and enabled. This may lead to having accounts addressed to totally different emails, that were verified. Note, that this way one is not able to take over any existing account (guest or normal one). The issue has been patched in Sylius 1.6.9, 1.7.9 and 1.8.3. As a workaround, you may resolve this issue on your own by creating a custom event listener, which will listen to the	https://github.com/Sylius/Sylius/security/advisories/GHSA-6gw4-x63h-5499	A-SYL-SYLI-031120/680

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sylius.customer.pre_update event. You can determine that email has been changed if customer email and user username are different. They are synchronized later on. Pay attention, to email changing behavior for administrators. You may need to skip this logic for them. In order to achieve this, you should either check master request path info, if it does not contain /admin prefix or adjust event triggered during customer update in the shop. You can find more information on how to customize the event here. **CVE ID : CVE-2020-15245**		
systeminformation					
systeminformation					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	26-Oct-20	6.5	This affects the package systeminformation before 4.27.11. This package is vulnerable to Command Injection. The attacker can concatenate curl's parameters to overwrite Javascript files and then execute any OS commands. **CVE ID : CVE-2020-7752**	https://github.com/sebhildebrandt/systeminformation/blob/master/lib/internet.js, https://github.com/sebhildebrandt/systeminformation/commit/931fecaec2c1a7dcc10457bb8cd552d08089da61, https://snyk.	A-SYS-SYST-031120/681

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				io/vuln/SNYK-JS-SYSTEMINFORMATION-1021909	
thembay					
greenmart					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Oct-20	4.3	The search functionality of the Greenmart theme 2.4.2 for WordPress is vulnerable to XSS. **CVE ID : CVE-2020-16140**	N/A	A-THE-GREE-031120/682
Tibco					
foresight_archive_and_retrieval_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Oct-20	6.5	The Transaction Insight reporting component of TIBCO Software Inc.'s TIBCO Foresight Archive and Retrieval System, TIBCO Foresight Archive and Retrieval System Healthcare Edition, TIBCO Foresight Operational Monitor, TIBCO Foresight Operational Monitor Healthcare Edition, TIBCO Foresight Transaction Insight, and TIBCO Foresight Transaction Insight Healthcare Edition contains a vulnerability that theoretically allows an authenticated attacker to perform SQL injection. Affected releases are TIBCO Software Inc.'s TIBCO Foresight Archive and	http://www.tibco.com/services/support/advisories	A-TIB-FORE-031120/683

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Retrieval System: versions 5.1.0 and below, version 5.2.0, TIBCO Foresight Archive and Retrieval System Healthcare Edition: versions 5.1.0 and below, version 5.2.0, TIBCO Foresight Operational Monitor: versions 5.1.0 and below, version 5.2.0, TIBCO Foresight Operational Monitor Healthcare Edition: versions 5.1.0 and below, version 5.2.0, TIBCO Foresight Transaction Insight: versions 5.1.0 and below, version 5.2.0, and TIBCO Foresight Transaction Insight Healthcare Edition: versions 5.1.0 and below, version 5.2.0. **CVE ID : CVE-2020-9417**		
foresight_operational_monitor					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Oct-20	6.5	The Transaction Insight reporting component of TIBCO Software Inc.'s TIBCO Foresight Archive and Retrieval System, TIBCO Foresight Archive and Retrieval System Healthcare Edition, TIBCO Foresight Operational Monitor, TIBCO Foresight Operational Monitor Healthcare Edition, TIBCO Foresight Transaction Insight, and TIBCO Foresight Transaction Insight Healthcare Edition contains a vulnerability that theoretically allows an	http://www.tibco.com/services/support/advisories	A-TIB-FORE-031120/684

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated attacker to perform SQL injection. Affected releases are TIBCO Software Inc.'s TIBCO Foresight Archive and Retrieval System: versions 5.1.0 and below, version 5.2.0, TIBCO Foresight Archive and Retrieval System Healthcare Edition: versions 5.1.0 and below, version 5.2.0, TIBCO Foresight Operational Monitor: versions 5.1.0 and below, version 5.2.0, TIBCO Foresight Operational Monitor Healthcare Edition: versions 5.1.0 and below, version 5.2.0, TIBCO Foresight Transaction Insight: versions 5.1.0 and below, version 5.2.0, and TIBCO Foresight Transaction Insight Healthcare Edition: versions 5.1.0 and below, version 5.2.0. **CVE ID : CVE-2020-9417**		
foresight_transaction_insight					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Oct-20	6.5	The Transaction Insight reporting component of TIBCO Software Inc.'s TIBCO Foresight Archive and Retrieval System, TIBCO Foresight Archive and Retrieval System Healthcare Edition, TIBCO Foresight Operational Monitor, TIBCO Foresight Operational Monitor Healthcare Edition, TIBCO Foresight Transaction	http://www.tibco.com/services/support/advisories	A-TIB-FORE-031120/685

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Insight, and TIBCO Foresight Transaction Insight Healthcare Edition contains a vulnerability that theoretically allows an authenticated attacker to perform SQL injection. Affected releases are TIBCO Software Inc.'s TIBCO Foresight Archive and Retrieval System: versions 5.1.0 and below, version 5.2.0, TIBCO Foresight Archive and Retrieval System Healthcare Edition: versions 5.1.0 and below, version 5.2.0, TIBCO Foresight Operational Monitor: versions 5.1.0 and below, version 5.2.0, TIBCO Foresight Operational Monitor Healthcare Edition: versions 5.1.0 and below, version 5.2.0, TIBCO Foresight Transaction Insight: versions 5.1.0 and below, version 5.2.0, and TIBCO Foresight Transaction Insight Healthcare Edition: versions 5.1.0 and below, version 5.2.0. **CVE ID : CVE-2020-9417**		
Tipsandtricks-hq					
simple_download_monitor					
Improper Neutralization of Input During Web Page Generation	21-Oct-20	4.3	Cross-site scripting vulnerability in Simple Download Monitor 3.8.8 and earlier allows remote attackers to inject an arbitrary script via	N/A	A-TIP-SIMP-031120/686

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			unspecified vectors. **CVE ID : CVE-2020-5650**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Oct-20	6.8	SQL injection vulnerability in Simple Download Monitor 3.8.8 and earlier allows remote attackers to execute arbitrary SQL commands via a specially crafted URL. **CVE ID : CVE-2020-5651**	N/A	A-TIP-SIMP-031120/687
trim_project					
trim					
N/A	27-Oct-20	5	All versions of package trim are vulnerable to Regular Expression Denial of Service (ReDoS) via trim(). **CVE ID : CVE-2020-7753**	N/A	A-TRI-TRIM-031120/688
ts.ed_project					
ts.ed					
Uncontrolled Resource Consumption	20-Oct-20	6.8	This affects the package @tsed/core before 5.65.7. This vulnerability relates to the deepExtend function which is used as part of the utils directory. Depending on if user input is provided, an attacker can overwrite and pollute the object prototype of a program. **CVE ID : CVE-2020-7748**	N/A	A-TS.-TS.E-031120/689
Ucweb					
uc_browser					
N/A	20-Oct-20	4.3	User Interface (UI) Misrepresentation of Critical Information vulnerability in the address bar of UCWeb's	N/A	A-UCW-UC_B-031120/690

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UC Browser allows an attacker to obfuscate the true source of data as presented in the browser. This issue affects UCWeb's UC Browser version 13.0.8 and prior versions. **CVE ID : CVE-2020-7363**		
N/A	20-Oct-20	4.3	User Interface (UI) Misrepresentation of Critical Information vulnerability in the address bar of UCWeb's UC Browser allows an attacker to obfuscate the true source of data as presented in the browser. This issue affects UCWeb's UC Browser version 13.0.8 and prior versions. **CVE ID : CVE-2020-7364**	N/A	A-UCW-UC_B-031120/691
veyon					
veyon					
Unquoted Search Path or Element	19-Oct-20	4.6	On Windows the Veyon Service before version 4.4.2 contains an unquoted service path vulnerability, allowing locally authenticated users with administrative privileges to run malicious executables with LocalSystem privileges. Since Veyon users (both students and teachers) usually don't have administrative privileges, this vulnerability is only dangerous in anyway unsafe setups. The problem has been fixed in version 4.4.2. As a workaround, the exploitation	https://github.com/veyon/veyon/security/advisories/GHSA-c8cc-x786-hqqp	A-VEY-VEYO-031120/692

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of the vulnerability can be prevented by revoking administrative privileges from all potentially untrustworthy users. **CVE ID : CVE-2020-15261**		
victor_cms_project					
victor_cms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	27-Oct-20	5	A SQL injection vulnerability exists in Victor CMS V1.0 in the cat_id parameter of the category.php file. This parameter can be used by sqlmap to obtain data information in the database. **CVE ID : CVE-2020-23945**	N/A	A-VIC-VICT-031120/693
vm-superio_project					
vm-superio					
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Oct-20	5	In vm-superio before 0.1.1, the serial console FIFO can grow to unlimited memory usage when data is sent to the input source (i.e., standard input). This behavior cannot be reproduced from the guest side. When no rate limiting is in place, the host can be subject to memory pressure, impacting all other VMs running on the same host. **CVE ID : CVE-2020-27173**	N/A	A-VM--VM-S-031120/694
Vmware					
horizon					
Improper Neutralization of Input During Web	23-Oct-20	3.5	VMware Horizon Server (7.x prior to 7.10.3 or 7.13.0) contains a Cross Site Scripting (XSS) vulnerability.	N/A	A-VMW-HORI-031120/695

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			Successful exploitation of this issue may allow an attacker to inject malicious script which will be executed. **CVE ID : CVE-2020-3997**		
vcenter_server					
Improper Certificate Validation	20-Oct-20	5.8	VMware vCenter Server (6.7 before 6.7u3, 6.6 before 6.5u3k) contains a session hijack vulnerability in the vCenter Server Appliance Management Interface update function due to a lack of certificate validation. A malicious actor with network positioning between vCenter Server and an update repository may be able to perform a session hijack when the vCenter Server Appliance Management Interface is used to download vCenter updates. **CVE ID : CVE-2020-3994**	N/A	A-VMW-VCEN-031120/696
workstation_player					
Out-of-bounds Write	20-Oct-20	4.9	VMware ESXi (7.0 before ESXi_7.0.1-0.0.16850804, 6.7 before ESXi670-202008101-SG, 6.5 before ESXi650-202007101-SG), Workstation (15.x), Fusion (11.x before 11.5.6) contain an out-of-bounds write vulnerability due to a time-of-check time-of-use issue in ACPI device. A malicious actor with administrative access to a virtual machine may be able to exploit this vulnerability to	N/A	A-VMW-WORK-031120/697

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crash the virtual machine's vmx process or corrupt hypervisor's memory heap. **CVE ID : CVE-2020-3982**		
nsx-t_data_center					
N/A	20-Oct-20	4.3	VMware NSX-T (3.x before 3.0.2, 2.5.x before 2.5.2.2.0) contains a security vulnerability that exists in the way it allows a KVM host to download and install packages from NSX manager. A malicious actor with MITM positioning may be able to exploit this issue to compromise the transport node. **CVE ID : CVE-2020-3993**	N/A	A-VMW-NSX--031120/698
velero					
N/A	22-Oct-20	2.1	Velero (prior to 1.4.3 and 1.5.2) in some instances doesn't properly manage volume identifiers which may result in information leakage to unauthorized users. **CVE ID : CVE-2020-3996**	N/A	A-VMW-VELE-031120/699
workstation					
Time-of-check Time-of-use (TOCTOU) Race Condition	20-Oct-20	3.5	VMware ESXi (7.0 before ESXi_7.0.1-0.0.16850804, 6.7 before ESXi670-202008101-SG, 6.5 before ESXi650-202007101-SG), Workstation (15.x), Fusion (11.x before 11.5.6) contain an out-of-bounds read vulnerability due to a time-of-check time-of-use issue in ACPI device. A malicious actor with	N/A	A-VMW-WORK-031120/700

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			administrative access to a virtual machine may be able to exploit this issue to leak memory from the vmx process. **CVE ID : CVE-2020-3981**		
Out-of-bounds Write	20-Oct-20	4.9	VMware ESXi (7.0 before ESXi_7.0.1-0.0.16850804, 6.7 before ESXi670-202008101-SG, 6.5 before ESXi650-202007101-SG), Workstation (15.x), Fusion (11.x before 11.5.6) contain an out-of-bounds write vulnerability due to a time-of-check time-of-use issue in ACPI device. A malicious actor with administrative access to a virtual machine may be able to exploit this vulnerability to crash the virtual machine's vmx process or corrupt hypervisor's memory heap. **CVE ID : CVE-2020-3982**	N/A	A-VMW-WORK-031120/701
Improper Release of Memory Before Removing Last Reference	20-Oct-20	3.5	In VMware ESXi (6.7 before ESXi670-201908101-SG, 6.5 before ESXi650-202007101-SG), Workstation (15.x before 15.1.0), Fusion (11.x before 11.1.0), the VMCI host drivers used by VMware hypervisors contain a memory leak vulnerability. A malicious actor with access to a virtual machine may be able to trigger a memory leak issue resulting in memory resource exhaustion on the hypervisor if the attack is sustained for extended periods of time.	N/A	A-VMW-WORK-031120/702

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3995		
fusion					
Time-of-check Time-of-use (TOCTOU) Race Condition	20-Oct-20	3.5	VMware ESXi (7.0 before ESXi_7.0.1-0.0.16850804, 6.7 before ESXi670-202008101-SG, 6.5 before ESXi650-202007101-SG), Workstation (15.x), Fusion (11.x before 11.5.6) contain an out-of-bounds read vulnerability due to a time-of-check time-of-use issue in ACPI device. A malicious actor with administrative access to a virtual machine may be able to exploit this issue to leak memory from the vmx process. **CVE ID : CVE-2020-3981**	N/A	A-VMW-FUSI-031120/703
Out-of-bounds Write	20-Oct-20	4.9	VMware ESXi (7.0 before ESXi_7.0.1-0.0.16850804, 6.7 before ESXi670-202008101-SG, 6.5 before ESXi650-202007101-SG), Workstation (15.x), Fusion (11.x before 11.5.6) contain an out-of-bounds write vulnerability due to a time-of-check time-of-use issue in ACPI device. A malicious actor with administrative access to a virtual machine may be able to exploit this vulnerability to crash the virtual machine's vmx process or corrupt hypervisor's memory heap. **CVE ID : CVE-2020-3982**	N/A	A-VMW-FUSI-031120/704
Improper Release of	20-Oct-20	3.5	In VMware ESXi (6.7 before ESXi670-201908101-SG, 6.5	N/A	A-VMW-FUSI-031120/705

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Before Removing Last Reference			before ESXi650-202007101-SG), Workstation (15.x before 15.1.0), Fusion (11.x before 11.1.0), the VMCI host drivers used by VMware hypervisors contain a memory leak vulnerability. A malicious actor with access to a virtual machine may be able to trigger a memory leak issue resulting in memory resource exhaustion on the hypervisor if the attack is sustained for extended periods of time. **CVE ID : CVE-2020-3995**		
cloud_foundation					
Time-of-check Time-of-use (TOCTOU) Race Condition	20-Oct-20	3.5	VMware ESXi (7.0 before ESXi_7.0.1-0.0.16850804, 6.7 before ESXi670-202008101-SG, 6.5 before ESXi650-202007101-SG), Workstation (15.x), Fusion (11.x before 11.5.6) contain an out-of-bounds read vulnerability due to a time-of-check time-of-use issue in ACPI device. A malicious actor with administrative access to a virtual machine may be able to exploit this issue to leak memory from the vmx process. **CVE ID : CVE-2020-3981**	N/A	A-VMW-CLOU-031120/706
Out-of-bounds Write	20-Oct-20	4.9	VMware ESXi (7.0 before ESXi_7.0.1-0.0.16850804, 6.7 before ESXi670-202008101-SG, 6.5 before ESXi650-202007101-SG), Workstation (15.x), Fusion (11.x before 11.5.6) contain an out-of-	N/A	A-VMW-CLOU-031120/707

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			bounds write vulnerability due to a time-of-check time-of-use issue in ACPI device. A malicious actor with administrative access to a virtual machine may be able to exploit this vulnerability to crash the virtual machine's vmx process or corrupt hypervisor's memory heap. **CVE ID : CVE-2020-3982**		
Use After Free	20-Oct-20	10	OpenSLP as used in VMware ESXi (7.0 before ESXi_7.0.1-0.0.16850804, 6.7 before ESXi670-202010401-SG, 6.5 before ESXi650-202010401-SG) has a use-after-free issue. A malicious actor residing in the management network who has access to port 427 on an ESXi machine may be able to trigger a use-after-free in the OpenSLP service resulting in remote code execution. **CVE ID : CVE-2020-3992**	N/A	A-VMW-CLOU-031120/708
N/A	20-Oct-20	4.3	VMware NSX-T (3.x before 3.0.2, 2.5.x before 2.5.2.2.0) contains a security vulnerability that exists in the way it allows a KVM host to download and install packages from NSX manager. A malicious actor with MITM positioning may be able to exploit this issue to compromise the transport node. **CVE ID : CVE-2020-3993**	N/A	A-VMW-CLOU-031120/709

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Certificate Validation	20-Oct-20	5.8	VMware vCenter Server (6.7 before 6.7u3, 6.6 before 6.5u3k) contains a session hijack vulnerability in the vCenter Server Appliance Management Interface update function due to a lack of certificate validation. A malicious actor with network positioning between vCenter Server and an update repository may be able to perform a session hijack when the vCenter Server Appliance Management Interface is used to download vCenter updates. **CVE ID : CVE-2020-3994**	N/A	A-VMW-CLOU-031120/710
Improper Release of Memory Before Removing Last Reference	20-Oct-20	3.5	In VMware ESXi (6.7 before ESXi670-201908101-SG, 6.5 before ESXi650-202007101-SG), Workstation (15.x before 15.1.0), Fusion (11.x before 11.1.0), the VMCI host drivers used by VMware hypervisors contain a memory leak vulnerability. A malicious actor with access to a virtual machine may be able to trigger a memory leak issue resulting in memory resource exhaustion on the hypervisor if the attack is sustained for extended periods of time. **CVE ID : CVE-2020-3995**	N/A	A-VMW-CLOU-031120/711
horizon_client					
N/A	16-Oct-20	3.6	VMware Horizon Client for Windows (5.x before 5.5.0) contains a denial-of-service vulnerability due to a file	N/A	A-VMW-HORI-031120/712

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system access control issue during install time. Successful exploitation of this issue may allow an attacker to overwrite certain admin privileged files through a symbolic link attack at install time. This will result into a denial-of-service condition on the machine where Horizon Client for Windows is installed. **CVE ID : CVE-2020-3991**		
Insufficiently Protected Credentials	23-Oct-20	4	VMware Horizon Client for Windows (5.x prior to 5.5.0) contains an information disclosure vulnerability. A malicious attacker with local privileges on the machine where Horizon Client for Windows is installed may be able to retrieve hashed credentials if the client crashes. **CVE ID : CVE-2020-3998**	N/A	A-VMW-HORI-031120/713
webpack-subresource-integrity_project					
webpack-subresource-integrity					
Insufficient Verification of Data Authenticity	19-Oct-20	5	In webpack-subresource-integrity before version 1.5.1, all dynamically loaded chunks receive an invalid integrity hash that is ignored by the browser, and therefore the browser cannot validate their integrity. This removes the additional level of protection offered by SRI for such chunks. Top-level chunks are unaffected. This	https://github.com/waysact/webpack-subresource-integrity/security/advisories/GHSA-4fc4-chg7-h8gh	A-WEB-WEBP-031120/714

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue is patched in version 1.5.1. **CVE ID : CVE-2020-15262**		
We-con					
levistudiou					
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	22-Oct-20	5	An XXE vulnerability exists within LeviStudioU Release Build 2019-09-21 and prior when processing parameter entities, which may allow file disclosure. **CVE ID : CVE-2020-25186**	N/A	A-WE--LEVI-031120/715
wire					
wire					
Improper Input Validation	16-Oct-20	6	In Wire before 3.20.x, `shell.openExternal` was used without checking the URL. This vulnerability allows an attacker to execute code on the victims machine by sending messages containing links with arbitrary protocols. The victim has to interact with the link and sees the URL that is opened. The issue was patched by implementing a helper function which checks if the URL's protocol is common. If it is common, the URL will be opened externally. If not, the URL will not be opened and a warning appears for the user informing them that a probably insecure URL was blocked from being executed. The issue is patched in Wire 3.20.x. More technical details	https://github.com/wireapp/wire-desktop/security/advisories/GHSA-5gpx-9976-ggpm	A-WIR-WIRE-031120/716

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			about exploitation are available in the linked advisory. **CVE ID : CVE-2020-15258**		
Wso2					
api_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Oct-20	4.3	WSO2 API Manager 3.1.0 and earlier has reflected XSS on the "publisher" component's admin interface. More precisely, it is possible to inject an XSS payload into the owner POST parameter, which does not filter user inputs. By putting an XSS payload in place of a valid Owner Name, a modal box appears that writes an error message concatenated to the injected payload (without any form of data encoding). This can also be exploited via CSRF. **CVE ID : CVE-2020-17454**	https://docs.wso2.com/display/Security/Security+Advisory+WSO2-2020-0843	A-WSO-API_-031120/717
Xwiki					
Xwiki					
Improper Control of Generation of Code ('Code Injection')	16-Oct-20	9	In XWiki before version 12.5 and 11.10.6, any user with SCRIPT right (EDIT right before XWiki 7.4) can gain access to the application server Servlet context which contains tools allowing to instantiate arbitrary Java objects and invoke methods that may lead to arbitrary code execution. This is patched in XWiki 12.5 and	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-5hv6-mh8q-q9v8	A-XWI-XWIK-031120/718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			XWiki 11.10.6. **CVE ID : CVE-2020-15252**		
Yandex					
yandex_browser					
Missing Authentication for Critical Function	20-Oct-20	4.3	User Interface (UI) Misrepresentation of Critical Information vulnerability in the address bar of the Yandex Browser allows an attacker to obfuscate the true source of data as presented in the browser. This issue affects the Yandex Browser version 20.8.3 and prior versions, and was fixed in version 20.8.4 released October 1, 2020. **CVE ID : CVE-2020-7369**	N/A	A-YAN-YAND-031120/719
Yourls					
Yourls					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Oct-20	3.5	Multiple Stored Cross Site Scripting (XSS) vulnerabilities exist in the YOURLS Admin Panel, Versions 1.5 - 1.7.10. An authenticated user must modify a PHP plugin with a malicious payload and upload it, resulting in multiple stored XSS issues. **CVE ID : CVE-2020-27388**	N/A	A-YOU-YOUR-031120/720
yubico					
yubihsm-shell					
Insufficient Session Expiration	19-Oct-20	5	An issue was discovered in the yh_create_session() function of yubihsm-shell through 2.0.2. The function does not explicitly check the	N/A	A-YUB-YUBI-031120/721

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			returned session id from the device. An invalid session id would lead to out-of-bounds read and write operations in the session array. This could be used by an attacker to cause a denial of service attack. **CVE ID : CVE-2020-24387**		
Improper Input Validation	19-Oct-20	5	An issue was discovered in the _send_secure_msg() function of yubihsm-shell through 2.0.2. The function does not validate the embedded length field of a message received from the device. This could lead to an oversized memcpy() call that will crash the running process. This could be used by an attacker to cause a denial of service. **CVE ID : CVE-2020-24388**	N/A	A-YUB-YUBI-031120/722
ZTE					
evdc					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-Oct-20	3.5	A ZTE product is impacted by an XSS vulnerability. The vulnerability is caused by the lack of correct verification of client data in the WEB module. By inserting malicious scripts into the web module, a remote attacker could trigger an XSS attack when the user browses the web page. Then the attacker could use the vulnerability to steal user cookies or destroy the page structure. This	N/A	A-ZTE-EVDC-031120/723

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affects: eVDC ZXCLOUD-iROSV6.03.04 **CVE ID : CVE-2020-6876**		
Operating System					
Apple					
iphone_os					
Origin Validation Error	27-Oct-20	7.2	A logic issue was addressed with improved validation. This issue is fixed in iCloud for Windows 7.17, iTunes 12.10.4 for Windows, iCloud for Windows 10.9.2, tvOS 13.3.1, Safari 13.0.5, iOS 13.3.1 and iPadOS 13.3.1. A DOM object context may not have had a unique security origin. **CVE ID : CVE-2020-3864**	N/A	O-APP-IPHO-031120/724
Out-of-bounds Read	27-Oct-20	9.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in watchOS 6.1.2, iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, macOS Catalina 10.15.3, Security Update 2020-001 Mojave, Security Update 2020-001 High Sierra. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-3880**	N/A	O-APP-IPHO-031120/725
N/A	22-Oct-20	2.1	An access issue was addressed with additional sandbox restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. A local user may be able	N/A	O-APP-IPHO-031120/726

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to view sensitive user information. **CVE ID : CVE-2020-3918**		
N/A	22-Oct-20	2.1	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. A sandboxed process may be able to circumvent sandbox restrictions. **CVE ID : CVE-2020-9772**	N/A	O-APP-IPHO-031120/727
N/A	22-Oct-20	5	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. Some websites may not have appeared in Safari Preferences. **CVE ID : CVE-2020-9787**	N/A	O-APP-IPHO-031120/728
N/A	22-Oct-20	4.6	A logic issue was addressed with improved validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5. An application may be able to gain elevated privileges. **CVE ID : CVE-2020-9854**	N/A	O-APP-IPHO-031120/729
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Oct-20	6.8	A command injection issue existed in Web Inspector. This issue was addressed with improved escaping. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3,	N/A	O-APP-IPHO-031120/730

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			iCloud for Windows 7.20. Copying a URL from Web Inspector may lead to command injection. **CVE ID : CVE-2020-9862**		
Improper Initialization	22-Oct-20	9.3	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9863**	N/A	O-APP-IPHO-031120/731
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Oct-20	6.8	A memory corruption issue was addressed by removing the vulnerable code. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. A malicious application may be able to break out of its sandbox. **CVE ID : CVE-2020-9865**	N/A	O-APP-IPHO-031120/732
Improper Certificate Validation	22-Oct-20	6.4	A certificate validation issue existed when processing administrator added certificates. This issue was addressed with improved certificate validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. An attacker may have been able to impersonate a trusted website using shared key material for an	N/A	O-APP-IPHO-031120/733

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			administrator added certificate. **CVE ID : CVE-2020-9868**		
Improper Input Validation	16-Oct-20	6.5	A logic issue was addressed with improved validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8. An attacker with memory write capability may be able to bypass pointer authentication codes and run arbitrary code. **CVE ID : CVE-2020-9870**	N/A	O-APP-IPHO-031120/734
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9871**	N/A	O-APP-IPHO-031120/735
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image	N/A	O-APP-IPHO-031120/736

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may lead to arbitrary code execution. **CVE ID : CVE-2020-9872**		
Out-of-bounds Read	22-Oct-20	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9873**	N/A	O-APP-IPHO-031120/737
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9874**	N/A	O-APP-IPHO-031120/738
Integer Overflow or Wraparound	22-Oct-20	6.8	An integer overflow was addressed through improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20.	N/A	O-APP-IPHO-031120/739

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9875**		
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Opening a maliciously crafted PDF file may lead to an unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9876**	N/A	O-APP-IPHO-031120/740
Out-of-bounds Read	22-Oct-20	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9877**	N/A	O-APP-IPHO-031120/741
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Oct-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a	N/A	O-APP-IPHO-031120/742

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9878**		
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9879**	N/A	O-APP-IPHO-031120/743
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Oct-20	6.8	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9880**	N/A	O-APP-IPHO-031120/744
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Oct-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, watchOS 6.2.8. Processing a maliciously crafted USD file may lead to	N/A	O-APP-IPHO-031120/745

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9881**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Oct-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, watchOS 6.2.8. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9882**	N/A	O-APP-IPHO-031120/746
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Oct-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9883**	N/A	O-APP-IPHO-031120/747
Out-of-bounds Write	16-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted audio file may lead to arbitrary code	N/A	O-APP-IPHO-031120/748

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2020-9884**		
Insufficient Verification of Data Authenticity	16-Oct-20	4.3	An issue existed in the handling of iMessage tapbacks. The issue was resolved with additional verification. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. A user that is removed from an iMessage group could rejoin the group. **CVE ID : CVE-2020-9885**	N/A	O-APP-IPHO-031120/749
Out-of-bounds Read	16-Oct-20	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9888**	N/A	O-APP-IPHO-031120/750
Out-of-bounds Write	16-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9889**	N/A	O-APP-IPHO-031120/751
Out-of-bounds Read	16-Oct-20	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS	N/A	O-APP-IPHO-031120/752

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9890**		
Out-of-bounds Read	16-Oct-20	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9891**	N/A	O-APP-IPHO-031120/753
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-Oct-20	9.3	Multiple memory corruption issues were addressed with improved state management. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. A malicious application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2020-9892**	N/A	O-APP-IPHO-031120/754
Use After Free	16-Oct-20	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A remote attacker may be able to cause unexpected application termination or	N/A	O-APP-IPHO-031120/755

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2020-9893**		
Out-of-bounds Read	16-Oct-20	4.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9894**	N/A	O-APP-IPHO-031120/756
Use After Free	16-Oct-20	7.5	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9895**	N/A	O-APP-IPHO-031120/757
N/A	22-Oct-20	7.5	This issue was addressed with improved entitlements. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6. A sandboxed process may be able to circumvent sandbox restrictions. **CVE ID : CVE-2020-9898**	N/A	O-APP-IPHO-031120/758

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Link Resolution Before File Access ('Link Following')	22-Oct-20	4.6	An issue existed within the path validation logic for symlinks. This issue was addressed with improved path sanitization. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2020-9900**	N/A	O-APP-IPHO-031120/759
Improper Link Resolution Before File Access ('Link Following')	22-Oct-20	4.6	An issue existed within the path validation logic for symlinks. This issue was addressed with improved path sanitization. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2020-9901**	N/A	O-APP-IPHO-031120/760
Out-of-bounds Read	22-Oct-20	7.1	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. A malicious application may be able to determine kernel memory layout. **CVE ID : CVE-2020-9902**	N/A	O-APP-IPHO-031120/761
Origin Validation Error	16-Oct-20	5	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.6 and iPadOS 13.6, Safari 13.1.2. A malicious attacker may cause Safari to suggest a password for the wrong	N/A	O-APP-IPHO-031120/762

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			domain. **CVE ID : CVE-2020-9903**		
N/A	22-Oct-20	9.3	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9904**	N/A	O-APP-IPHO-031120/763
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Oct-20	5	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8. A remote attacker may be able to cause a denial of service. **CVE ID : CVE-2020-9905**	N/A	O-APP-IPHO-031120/764
Improper Input Validation	22-Oct-20	9.4	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, watchOS 6.2.8. A remote attacker may be able to cause unexpected system termination or corrupt kernel memory. **CVE ID : CVE-2020-9906**	N/A	O-APP-IPHO-031120/765
Improper Restriction of Operations within the Bounds of a	16-Oct-20	9.3	A memory corruption issue was addressed by removing the vulnerable code. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8. An application may be able to	N/A	O-APP-IPHO-031120/766

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9907**		
Out-of-bounds Read	16-Oct-20	4.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8. An attacker that has already achieved kernel code execution may be able to bypass kernel memory mitigations. **CVE ID : CVE-2020-9909**	N/A	O-APP-IPHO-031120/767
Improper Authentication	16-Oct-20	6.5	Multiple issues were addressed with improved logic. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A malicious attacker with arbitrary read and write capability may be able to bypass Pointer Authentication. **CVE ID : CVE-2020-9910**	N/A	O-APP-IPHO-031120/768
N/A	16-Oct-20	5	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.6 and iPadOS 13.6, Safari 13.1.2. An issue in Safari Reader mode may allow a remote attacker to bypass the Same Origin Policy. **CVE ID : CVE-2020-9911**	N/A	O-APP-IPHO-031120/769
Improper Input	16-Oct-20	5	An input validation issue existed in Bluetooth. This	N/A	O-APP-IPHO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			issue was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8. An attacker in a privileged network position may be able to perform denial of service attack using malformed Bluetooth packets. **CVE ID : CVE-2020-9914**		031120/770
N/A	16-Oct-20	4.3	An access issue existed in Content Security Policy. This issue was addressed with improved access restrictions. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing maliciously crafted web content may prevent Content Security Policy from being enforced. **CVE ID : CVE-2020-9915**	N/A	O-APP-IPHO-031120/771
N/A	16-Oct-20	5	A URL Unicode encoding issue was addressed with improved state management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A malicious attacker may be able to conceal the destination of a URL. **CVE ID : CVE-2020-9916**	N/A	O-APP-IPHO-031120/772
N/A	16-Oct-20	5	This issue was addressed	N/A	O-APP-IPHO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with improved checks. This issue is fixed in iOS 13.6 and iPadOS 13.6. A remote attacker may be able to cause a denial of service. **CVE ID : CVE-2020-9917**		031120/773
Out-of-bounds Read	16-Oct-20	10	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. A remote attacker may be able to cause unexpected system termination or corrupt kernel memory. **CVE ID : CVE-2020-9918**	N/A	O-APP-IPHO-031120/774
Out-of-bounds Write	22-Oct-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9919**	N/A	O-APP-IPHO-031120/775
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Oct-20	6.4	A path handling issue was addressed with improved validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, watchOS 6.2.8. A malicious mail server may overwrite arbitrary mail files. **CVE ID : CVE-2020-9920**	N/A	O-APP-IPHO-031120/776

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Oct-20	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, watchOS 6.2.8. A malicious application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2020-9923**	N/A	O-APP-IPHO-031120/777
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-20	4.3	A logic issue was addressed with improved state management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2020-9925**	N/A	O-APP-IPHO-031120/778
Improper Input Validation	16-Oct-20	5	A denial of service issue was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6. A remote attacker may cause an unexpected application termination. **CVE ID : CVE-2020-9931**	N/A	O-APP-IPHO-031120/779
Incorrect Authorization	16-Oct-20	4.3	An authorization issue was addressed with improved state management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8. A malicious application may be able to read sensitive location	N/A	O-APP-IPHO-031120/780

CVSS Scoring Scale	0-1	1-2	2-3	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. **CVE ID : CVE-2020-9933**		
N/A	16-Oct-20	2.1	An issue existed in the handling of environment variables. This issue was addressed with improved validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6. A local user may be able to view sensitive user information. **CVE ID : CVE-2020-9934**	N/A	O-APP-IPHO-031120/781
Out-of-bounds Write	16-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9936**	N/A	O-APP-IPHO-031120/782
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution.	N/A	O-APP-IPHO-031120/783

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
			CVE ID : CVE-2020-9937		
Out-of-bounds Read	22-Oct-20	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9938**	N/A	O-APP-IPHO-031120/784
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Oct-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9940**	N/A	O-APP-IPHO-031120/785
Improper Locking	16-Oct-20	4.6	This issue was addressed with improved checks. This issue is fixed in iOS 14.0 and iPadOS 14.0, watchOS 7.0. The screen lock may not engage after the specified time period. **CVE ID : CVE-2020-9946**	N/A	O-APP-IPHO-031120/786
Improper Neutralization of Input During Web Page	16-Oct-20	4.3	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 14.0 and iPadOS 14.0, tvOS 14.0, watchOS 7.0,	N/A	O-APP-IPHO-031120/787

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Safari 14.0, iCloud for Windows 11.4, iCloud for Windows 7.21. Processing maliciously crafted web content may lead to a cross site scripting attack. **CVE ID : CVE-2020-9952**		
Out-of-bounds Write	16-Oct-20	9.3	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 14.0 and iPadOS 14.0. An application may be able to cause unexpected system termination or write kernel memory. **CVE ID : CVE-2020-9958**	N/A	O-APP-IPHO-031120/788
Improper Locking	16-Oct-20	2.1	A lock screen issue allowed access to messages on a locked device. This issue was addressed with improved state management. This issue is fixed in iOS 14.0 and iPadOS 14.0. A person with physical access to an iOS device may be able to view notification contents from the lockscreen. **CVE ID : CVE-2020-9959**	N/A	O-APP-IPHO-031120/789
Improper Initialization	16-Oct-20	4.9	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 14.0 and iPadOS 14.0. A local user may be able to read kernel memory. **CVE ID : CVE-2020-9964**	N/A	O-APP-IPHO-031120/790
N/A	16-Oct-20	4.3	A logic issue was addressed with improved restrictions.	N/A	O-APP-IPHO-

CVSS Scoring Scale	0-1	1-2	2-3	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 issue is fixed in iOS 14.0 and iPadOS 14.0, macOS Catalina 10.15.7, tvOS 14.0, watchOS 7.0. A malicious application may be able to access restricted files. **CVE ID : CVE-2020-9968**		031120/791
Out-of-bounds Read	27-Oct-20	9.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Catalina 10.15.7, Security Update 2020-005 High Sierra, Security Update 2020-005 Mojave, iOS 14.0 and iPadOS 14.0. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9973**	N/A	O-APP-IPHO-031120/792
Information Exposure	16-Oct-20	4.3	A logic issue was addressed with improved state management. This issue is fixed in iOS 14.0 and iPadOS 14.0, tvOS 14.0, watchOS 7.0. A malicious application may be able to leak sensitive user information. **CVE ID : CVE-2020-9976**	N/A	O-APP-IPHO-031120/793
N/A	27-Oct-20	2.1	A trust issue was addressed by removing a legacy API. This issue is fixed in iOS 14.0 and iPadOS 14.0, tvOS 14.0. An attacker may be able to misuse a trust relationship to download malicious content. **CVE ID : CVE-2020-9979**	N/A	O-APP-IPHO-031120/794

CVSS Scoring Scale	0-1	1-2	2-3	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	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted font file may lead to arbitrary code execution. **CVE ID : CVE-2020-9980**	N/A	O-APP-IPHO-031120/795
Out-of-bounds Read	22-Oct-20	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9984**	N/A	O-APP-IPHO-031120/796
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Oct-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, watchOS 6.2.8. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9985**	N/A	O-APP-IPHO-031120/797
N/A	16-Oct-20	9.3	This issue was addressed by encrypting communications over the network to devices	N/A	O-APP-IPHO-031120/798

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
			running iOS 14, iPadOS 14, tvOS 14, and watchOS 7. This issue is fixed in iOS 14.0 and iPadOS 14.0, Xcode 12.0. An attacker in a privileged network position may be able to execute arbitrary code on a paired device during a debug session over the network. **CVE ID : CVE-2020-9992**		
N/A	22-Oct-20	5.8	A path handling issue was addressed with improved validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to overwrite arbitrary files. **CVE ID : CVE-2020-9994**	N/A	O-APP-IPHO-031120/799
mac_os_x					
Time-of-check Time-of-use (TOCTOU) Race Condition	20-Oct-20	3.5	VMware ESXi (7.0 before ESXi_7.0.1-0.0.16850804, 6.7 before ESXi670-202008101-SG, 6.5 before ESXi650-202007101-SG), Workstation (15.x), Fusion (11.x before 11.5.6) contain an out-of-bounds read vulnerability due to a time-of-check time-of-use issue in ACPI device. A malicious actor with administrative access to a virtual machine may be able to exploit this issue to leak memory from the vmx process. **CVE ID : CVE-2020-3981**	N/A	O-APP-MAC_-031120/800
Out-of-	20-Oct-20	4.9	VMware ESXi (7.0 before	N/A	O-APP-MAC_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			ESXi_7.0.1-0.0.16850804, 6.7 before ESXi670-202008101-SG, 6.5 before ESXi650-202007101-SG), Workstation (15.x), Fusion (11.x before 11.5.6) contain an out-of-bounds write vulnerability due to a time-of-check time-of-use issue in ACPI device. A malicious actor with administrative access to a virtual machine may be able to exploit this vulnerability to crash the virtual machine's vmx process or corrupt hypervisor's memory heap. **CVE ID : CVE-2020-3982**		031120/801
N/A	27-Oct-20	5.8	An access issue was addressed with improved access restrictions. This issue is fixed in macOS Catalina 10.15.3, Security Update 2020-001 Mojave, Security Update 2020-001 High Sierra. A malicious application may be able to overwrite arbitrary files. **CVE ID : CVE-2020-3855**	N/A	O-APP-MAC_-031120/802
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Oct-20	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15.3, Security Update 2020-001 Mojave, Security Update 2020-001 High Sierra. An application may be able to execute arbitrary code with system privileges.	N/A	O-APP-MAC_-031120/803

CVSS Scoring Scale	0-1	1-2	2-3	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-2020-3863		
Out-of-bounds Read	27-Oct-20	9.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in watchOS 6.1.2, iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, macOS Catalina 10.15.3, Security Update 2020-001 Mojave, Security Update 2020-001 High Sierra. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-3880**	N/A	O-APP-MAC_-031120/804
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-Oct-20	4.6	A memory corruption issue was addressed with improved validation. This issue is fixed in macOS Catalina 10.15.4. An application may be able to gain elevated privileges. **CVE ID : CVE-2020-3898**	N/A	O-APP-MAC_-031120/805
N/A	22-Oct-20	4.6	A path handling issue was addressed with improved validation. This issue is fixed in macOS Catalina 10.15.4. A malicious application may be able to overwrite arbitrary files. **CVE ID : CVE-2020-3915**	N/A	O-APP-MAC_-031120/806
N/A	22-Oct-20	2.1	An access issue was addressed with additional sandbox restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. A local user may be able to view sensitive user information.	N/A	O-APP-MAC_-031120/807

CVSS Scoring Scale	0-1	1-2	2-3	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-2020-3918		
Improper Release of Memory Before Removing Last Reference	20-Oct-20	3.5	In VMware ESXi (6.7 before ESXi670-201908101-SG, 6.5 before ESXi650-202007101-SG), Workstation (15.x before 15.1.0), Fusion (11.x before 11.1.0), the VMCI host drivers used by VMware hypervisors contain a memory leak vulnerability. A malicious actor with access to a virtual machine may be able to trigger a memory leak issue resulting in memory resource exhaustion on the hypervisor if the attack is sustained for extended periods of time. **CVE ID : CVE-2020-3995**	N/A	O-APP-MAC_-031120/808
N/A	22-Oct-20	3.6	This issue was addressed with a new entitlement. This issue is fixed in macOS Catalina 10.15.4. A user may gain access to protected parts of the file system. **CVE ID : CVE-2020-9771**	N/A	O-APP-MAC_-031120/809
N/A	22-Oct-20	2.1	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. A sandboxed process may be able to circumvent sandbox restrictions. **CVE ID : CVE-2020-9772**	N/A	O-APP-MAC_-031120/810
Missing Encryption of Sensitive Data	27-Oct-20	5	An issue existed with Siri Suggestions access to encrypted data. The issue was fixed by limiting access	N/A	O-APP-MAC_-031120/811

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
			to encrypted data. This issue is fixed in macOS Catalina 10.15.3, Security Update 2020-001 Mojave, Security Update 2020-001 High Sierra. Encrypted data may be inappropriately accessed. **CVE ID : CVE-2020-9774**		
Out-of-bounds Read	22-Oct-20	6.6	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.4. A local user may be able to cause unexpected system termination or read kernel memory. **CVE ID : CVE-2020-9779**	N/A	O-APP-MAC_-031120/812
N/A	27-Oct-20	4.3	This issue was addressed with improved checks This issue is fixed in macOS Catalina 10.15.4, Security Update 2020-002 Mojave, Security Update 2020-002 High Sierra. An application may be able to trigger a sysdiagnose. **CVE ID : CVE-2020-9786**	N/A	O-APP-MAC_-031120/813
N/A	22-Oct-20	5	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. Some websites may not have appeared in Safari Preferences. **CVE ID : CVE-2020-9787**	N/A	O-APP-MAC_-031120/814
Concurrent Execution using Shared	22-Oct-20	6.9	A race condition was addressed with improved state handling. This issue is	N/A	O-APP-MAC_-031120/815

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			fixed in macOS Catalina 10.15.5. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9796**		
Out-of-bounds Read	16-Oct-20	9.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Catalina 10.15.6. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9799**	N/A	O-APP-MAC_-031120/816
N/A	22-Oct-20	4.6	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Catalina 10.15.5. A person with physical access to a Mac may be able to bypass Login Window. **CVE ID : CVE-2020-9810**	N/A	O-APP-MAC_-031120/817
Out-of-bounds Read	22-Oct-20	5	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.4. A remote attacker may be able to leak sensitive user information. **CVE ID : CVE-2020-9828**	N/A	O-APP-MAC_-031120/818
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-Oct-20	6.8	A memory corruption issue was addressed with improved validation. This issue is fixed in macOS Catalina 10.15.4. A malicious application may be able to determine kernel memory layout.	N/A	O-APP-MAC_-031120/819

CVSS Scoring Scale	0-1	1-2	2-3	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-2020-9853		
N/A	22-Oct-20	4.6	A logic issue was addressed with improved validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5. An application may be able to gain elevated privileges. **CVE ID : CVE-2020-9854**	N/A	O-APP-MAC_-031120/820
N/A	27-Oct-20	4.3	An issue existed in the parsing of URLs. This issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.5, Security Update 2020-003 Mojave, Security Update 2020-003 High Sierra. A malicious website may be able to exfiltrate autofilled data in Safari. **CVE ID : CVE-2020-9857**	N/A	O-APP-MAC_-031120/821
Improper Initialization	22-Oct-20	9.3	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9863**	N/A	O-APP-MAC_-031120/822
N/A	16-Oct-20	10	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Catalina 10.15.6. An application may be able to execute arbitrary code with	N/A	O-APP-MAC_-031120/823

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
			kernel privileges. **CVE ID : CVE-2020-9864**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Oct-20	6.8	A memory corruption issue was addressed by removing the vulnerable code. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. A malicious application may be able to break out of its sandbox. **CVE ID : CVE-2020-9865**	N/A	O-APP-MAC_-031120/824
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	27-Oct-20	7.5	A buffer overflow was addressed with improved bounds checking. This issue is fixed in macOS Catalina 10.15.6, Security Update 2020-004 Mojave, Security Update 2020-004 High Sierra. A buffer overflow may result in arbitrary code execution. **CVE ID : CVE-2020-9866**	N/A	O-APP-MAC_-031120/825
Improper Certificate Validation	22-Oct-20	6.4	A certificate validation issue existed when processing administrator added certificates. This issue was addressed with improved certificate validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. An attacker may have been able to impersonate a trusted website using shared key material for an administrator added certificate. **CVE ID : CVE-2020-9868**	N/A	O-APP-MAC_-031120/826

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
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-Oct-20	5	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15.6. A remote attacker may cause an unexpected application termination. **CVE ID : CVE-2020-9869**	N/A	O-APP-MAC_-031120/827
Improper Input Validation	16-Oct-20	6.5	A logic issue was addressed with improved validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8. An attacker with memory write capability may be able to bypass pointer authentication codes and run arbitrary code. **CVE ID : CVE-2020-9870**	N/A	O-APP-MAC_-031120/828
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9871**	N/A	O-APP-MAC_-031120/829
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS	N/A	O-APP-MAC_-031120/830

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
			Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9872**		
Out-of-bounds Read	22-Oct-20	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9873**	N/A	O-APP-MAC_-031120/831
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9874**	N/A	O-APP-MAC_-031120/832
Integer Overflow or Wraparound	22-Oct-20	6.8	An integer overflow was addressed through improved input validation. This issue is	N/A	O-APP-MAC_-031120/833

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9875**		
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Opening a maliciously crafted PDF file may lead to an unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9876**	N/A	O-APP-MAC_-031120/834
Out-of-bounds Read	22-Oct-20	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9877**	N/A	O-APP-MAC_-031120/835
Buffer Copy	16-Oct-20	6.8	A buffer overflow issue was	N/A	O-APP-MAC_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9878**		031120/836
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9879**	N/A	O-APP-MAC_-031120/837
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Oct-20	6.8	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9880**	N/A	O-APP-MAC_-031120/838
Buffer Copy without	22-Oct-20	6.8	A buffer overflow issue was addressed with improved	N/A	O-APP-MAC_-031120/839

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, watchOS 6.2.8. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9881**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Oct-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, watchOS 6.2.8. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9882**	N/A	O-APP-MAC_-031120/840
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Oct-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9883**	N/A	O-APP-MAC_-031120/841
Out-of-bounds Write	16-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking.	N/A	O-APP-MAC_-031120/842

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9884**		
Insufficient Verification of Data Authenticity	16-Oct-20	4.3	An issue existed in the handling of iMessage tapbacks. The issue was resolved with additional verification. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. A user that is removed from an iMessage group could rejoin the group. **CVE ID : CVE-2020-9885**	N/A	O-APP-MAC_-031120/843
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-Oct-20	6.8	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.6. Viewing a maliciously crafted JPEG file may lead to arbitrary code execution. **CVE ID : CVE-2020-9887**	N/A	O-APP-MAC_-031120/844
Out-of-bounds Read	16-Oct-20	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9888**	N/A	O-APP-MAC_-031120/845

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9889**	N/A	O-APP-MAC_-031120/846
Out-of-bounds Read	16-Oct-20	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9890**	N/A	O-APP-MAC_-031120/847
Out-of-bounds Read	16-Oct-20	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9891**	N/A	O-APP-MAC_-031120/848
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-Oct-20	9.3	Multiple memory corruption issues were addressed with improved state management. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. A malicious application may be able to	N/A	O-APP-MAC_-031120/849

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code with system privileges. **CVE ID : CVE-2020-9892**		
N/A	22-Oct-20	7.5	This issue was addressed with improved entitlements. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6. A sandboxed process may be able to circumvent sandbox restrictions. **CVE ID : CVE-2020-9898**	N/A	O-APP-MAC_-031120/850
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-Oct-20	9.3	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.6. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9899**	N/A	O-APP-MAC_-031120/851
Improper Link Resolution Before File Access ('Link Following')	22-Oct-20	4.6	An issue existed within the path validation logic for symlinks. This issue was addressed with improved path sanitization. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2020-9900**	N/A	O-APP-MAC_-031120/852
Improper Link Resolution Before File Access ('Link Following')	22-Oct-20	4.6	An issue existed within the path validation logic for symlinks. This issue was addressed with improved path sanitization. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6,	N/A	O-APP-MAC_-031120/853

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			tvOS 13.4.8. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2020-9901**		
Out-of-bounds Read	22-Oct-20	7.1	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. A malicious application may be able to determine kernel memory layout. **CVE ID : CVE-2020-9902**	N/A	O-APP-MAC_-031120/854
N/A	22-Oct-20	9.3	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9904**	N/A	O-APP-MAC_-031120/855
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Oct-20	5	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8. A remote attacker may be able to cause a denial of service. **CVE ID : CVE-2020-9905**	N/A	O-APP-MAC_-031120/856
Improper Input Validation	22-Oct-20	9.4	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS	N/A	O-APP-MAC_-031120/857

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Catalina 10.15.6, watchOS 6.2.8. A remote attacker may be able to cause unexpected system termination or corrupt kernel memory. **CVE ID : CVE-2020-9906**		
Out-of-bounds Read	22-Oct-20	6.6	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.6. A local user may be able to cause unexpected system termination or read kernel memory. **CVE ID : CVE-2020-9908**	N/A	O-APP-MAC_-031120/858
N/A	16-Oct-20	2.1	This issue was addressed with improved data protection. This issue is fixed in macOS Catalina 10.15.6. A local user may be able to leak sensitive user information. **CVE ID : CVE-2020-9913**	N/A	O-APP-MAC_-031120/859
Out-of-bounds Read	16-Oct-20	10	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. A remote attacker may be able to cause unexpected system termination or corrupt kernel memory. **CVE ID : CVE-2020-9918**	N/A	O-APP-MAC_-031120/860
Out-of-bounds Write	22-Oct-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for	N/A	O-APP-MAC_-031120/861

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
			Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9919**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Oct-20	6.4	A path handling issue was addressed with improved validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, watchOS 6.2.8. A malicious mail server may overwrite arbitrary mail files. **CVE ID : CVE-2020-9920**	N/A	O-APP-MAC_-031120/862
Time-of-check Time-of-use (TOCTOU) Race Condition	22-Oct-20	6.9	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15.6. A malicious application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2020-9921**	N/A	O-APP-MAC_-031120/863
N/A	22-Oct-20	5	A logic issue was addressed with improved state management. This issue is fixed in macOS Catalina 10.15.6. A remote attacker may be able to cause a denial of service. **CVE ID : CVE-2020-9924**	N/A	O-APP-MAC_-031120/864
Out-of-bounds Write	22-Oct-20	7.2	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.6. An application may be able to	N/A	O-APP-MAC_-031120/865

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9927**		
N/A	22-Oct-20	9.3	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15.6. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9928**	N/A	O-APP-MAC_-031120/866
N/A	22-Oct-20	6.6	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15.6. A local user may be able to cause unexpected system termination or read kernel memory. **CVE ID : CVE-2020-9929**	N/A	O-APP-MAC_-031120/867
N/A	16-Oct-20	2.1	An issue existed in the handling of environment variables. This issue was addressed with improved validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6. A local user may be able to view sensitive user information. **CVE ID : CVE-2020-9934**	N/A	O-APP-MAC_-031120/868
N/A	22-Oct-20	4	A logic issue was addressed with improved state management. This issue is fixed in macOS Catalina 10.15.6. A user may be unexpectedly logged in to	N/A	O-APP-MAC_-031120/869

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			another user's account. **CVE ID : CVE-2020-9935**		
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9937**	N/A	O-APP-MAC_-031120/870
Out-of-bounds Read	22-Oct-20	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9938**	N/A	O-APP-MAC_-031120/871
Time-of-check Time-of-use (TOCTOU) Race Condition	22-Oct-20	4.4	This issue was addressed with improved checks. This issue is fixed in macOS Catalina 10.15.6. A local user may be able to load unsigned kernel extensions. **CVE ID : CVE-2020-9939**	N/A	O-APP-MAC_-031120/872
Buffer Copy without Checking	22-Oct-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue	N/A	O-APP-MAC_-031120/873

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9940**		
N/A	27-Oct-20	5	This issue was addressed with improved checks. This issue is fixed in macOS Catalina 10.15.7, Security Update 2020-005 High Sierra, Security Update 2020-005 Mojave. A remote attacker may be able to unexpectedly alter application state. **CVE ID : CVE-2020-9941**	N/A	O-APP-MAC_-031120/874
Out-of-bounds Read	27-Oct-20	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.7, Security Update 2020-005 High Sierra, Security Update 2020-005 Mojave. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9961**	N/A	O-APP-MAC_-031120/875
N/A	16-Oct-20	4.3	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 14.0 and iPadOS 14.0, macOS Catalina 10.15.7, tvOS 14.0, watchOS 7.0. A malicious application may be able to access restricted files.	N/A	O-APP-MAC_-031120/876

CVSS Scoring Scale	0-1	1-2	2-3	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-2020-9968		
Out-of-bounds Read	27-Oct-20	9.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Catalina 10.15.7, Security Update 2020-005 High Sierra, Security Update 2020-005 Mojave, iOS 14.0 and iPadOS 14.0. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9973**	N/A	O-APP-MAC_-031120/877
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted font file may lead to arbitrary code execution. **CVE ID : CVE-2020-9980**	N/A	O-APP-MAC_-031120/878
Out-of-bounds Read	22-Oct-20	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9984**	N/A	O-APP-MAC_-031120/879

CVSS Scoring Scale	0-1	1-2	2-3	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')	22-Oct-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, watchOS 6.2.8. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9985**	N/A	O-APP-MAC_-031120/880
N/A	22-Oct-20	4.3	A file access issue existed with certain home folder files. This was addressed with improved access restrictions. This issue is fixed in macOS Catalina 10.15.7. A malicious application may be able to read sensitive location information. **CVE ID : CVE-2020-9986**	N/A	O-APP-MAC_-031120/881
Time-of-check Time-of-use (TOCTOU) Race Condition	22-Oct-20	6.9	A race condition was addressed with additional validation. This issue is fixed in macOS Catalina 10.15.6. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9990**	N/A	O-APP-MAC_-031120/882
N/A	22-Oct-20	5.8	A path handling issue was addressed with improved validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to overwrite arbitrary files.	N/A	O-APP-MAC_-031120/883

CVSS Scoring Scale	0-1	1-2	2-3	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-2020-9994		
N/A	22-Oct-20	4.3	An information disclosure issue was addressed with improved state management. This issue is fixed in macOS Catalina 10.15.6, watchOS 6.2.8. A malicious application may disclose restricted memory. **CVE ID : CVE-2020-9997**	N/A	O-APP-MAC_-031120/884
watchos					
Out-of-bounds Read	27-Oct-20	9.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in watchOS 6.1.2, iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, macOS Catalina 10.15.3, Security Update 2020-001 Mojave, Security Update 2020-001 High Sierra. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-3880**	N/A	O-APP-WATC-031120/885
N/A	22-Oct-20	2.1	An access issue was addressed with additional sandbox restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. A local user may be able to view sensitive user information. **CVE ID : CVE-2020-3918**	N/A	O-APP-WATC-031120/886
N/A	22-Oct-20	2.1	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4,	N/A	O-APP-WATC-031120/887

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			watchOS 6.2. A sandboxed process may be able to circumvent sandbox restrictions. **CVE ID : CVE-2020-9772**		
N/A	22-Oct-20	5	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. Some websites may not have appeared in Safari Preferences. **CVE ID : CVE-2020-9787**	N/A	O-APP-WATC-031120/888
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Oct-20	6.8	A command injection issue existed in Web Inspector. This issue was addressed with improved escaping. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Copying a URL from Web Inspector may lead to command injection. **CVE ID : CVE-2020-9862**	N/A	O-APP-WATC-031120/889
Improper Initialization	22-Oct-20	9.3	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9863**	N/A	O-APP-WATC-031120/890

CVSS Scoring Scale	0-1	1-2	2-3	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	16-Oct-20	6.8	A memory corruption issue was addressed by removing the vulnerable code. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. A malicious application may be able to break out of its sandbox. **CVE ID : CVE-2020-9865**	N/A	O-APP-WATC-031120/891
Improper Certificate Validation	22-Oct-20	6.4	A certificate validation issue existed when processing administrator added certificates. This issue was addressed with improved certificate validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. An attacker may have been able to impersonate a trusted website using shared key material for an administrator added certificate. **CVE ID : CVE-2020-9868**	N/A	O-APP-WATC-031120/892
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution.	N/A	O-APP-WATC-031120/893

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9871		
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9872**	N/A	O-APP-WATC-031120/894
Out-of-bounds Read	22-Oct-20	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9873**	N/A	O-APP-WATC-031120/895
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code	N/A	O-APP-WATC-031120/896

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2020-9874**		
Integer Overflow or Wraparound	22-Oct-20	6.8	An integer overflow was addressed through improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9875**	N/A	O-APP-WATC-031120/897
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Opening a maliciously crafted PDF file may lead to an unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9876**	N/A	O-APP-WATC-031120/898
Out-of-bounds Read	22-Oct-20	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20.	N/A	O-APP-WATC-031120/899

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9877**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Oct-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9878**	N/A	O-APP-WATC-031120/900
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9879**	N/A	O-APP-WATC-031120/901
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Oct-20	6.8	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted USD file may lead to unexpected application	N/A	O-APP-WATC-031120/902

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			termination or arbitrary code execution. **CVE ID : CVE-2020-9880**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Oct-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, watchOS 6.2.8. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9881**	N/A	O-APP-WATC-031120/903
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Oct-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, watchOS 6.2.8. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9882**	N/A	O-APP-WATC-031120/904
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Oct-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code	N/A	O-APP-WATC-031120/905

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2020-9883**		
Out-of-bounds Write	16-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9884**	N/A	O-APP-WATC-031120/906
Insufficient Verification of Data Authenticity	16-Oct-20	4.3	An issue existed in the handling of iMessage tapbacks. The issue was resolved with additional verification. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. A user that is removed from an iMessage group could rejoin the group. **CVE ID : CVE-2020-9885**	N/A	O-APP-WATC-031120/907
Out-of-bounds Read	16-Oct-20	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9888**	N/A	O-APP-WATC-031120/908
Out-of-bounds Write	16-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6	N/A	O-APP-WATC-031120/909

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9889**		
Out-of-bounds Read	16-Oct-20	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9890**	N/A	O-APP-WATC-031120/910
Out-of-bounds Read	16-Oct-20	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9891**	N/A	O-APP-WATC-031120/911
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-Oct-20	9.3	Multiple memory corruption issues were addressed with improved state management. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. A malicious application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2020-9892**	N/A	O-APP-WATC-031120/912

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
Use After Free	16-Oct-20	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9893**	N/A	O-APP-WATC-031120/913
Out-of-bounds Read	16-Oct-20	4.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9894**	N/A	O-APP-WATC-031120/914
Use After Free	16-Oct-20	7.5	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A remote attacker may be able to cause unexpected application termination or	N/A	O-APP-WATC-031120/915

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2020-9895**		
Improper Link Resolution Before File Access ('Link Following')	22-Oct-20	4.6	An issue existed within the path validation logic for symlinks. This issue was addressed with improved path sanitization. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2020-9900**	N/A	O-APP-WATC-031120/916
Out-of-bounds Read	22-Oct-20	7.1	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. A malicious application may be able to determine kernel memory layout. **CVE ID : CVE-2020-9902**	N/A	O-APP-WATC-031120/917
N/A	22-Oct-20	9.3	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9904**	N/A	O-APP-WATC-031120/918
Improper Input Validation	22-Oct-20	9.4	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS	N/A	O-APP-WATC-031120/919

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
			Catalina 10.15.6, watchOS 6.2.8. A remote attacker may be able to cause unexpected system termination or corrupt kernel memory. **CVE ID : CVE-2020-9906**		
Out-of-bounds Read	16-Oct-20	4.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8. An attacker that has already achieved kernel code execution may be able to bypass kernel memory mitigations. **CVE ID : CVE-2020-9909**	N/A	O-APP-WATC-031120/920
Improper Authentication	16-Oct-20	6.5	Multiple issues were addressed with improved logic. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A malicious attacker with arbitrary read and write capability may be able to bypass Pointer Authentication. **CVE ID : CVE-2020-9910**	N/A	O-APP-WATC-031120/921
N/A	16-Oct-20	4.3	An access issue existed in Content Security Policy. This issue was addressed with improved access restrictions. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows,	N/A	O-APP-WATC-031120/922

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			iCloud for Windows 11.3, iCloud for Windows 7.20. Processing maliciously crafted web content may prevent Content Security Policy from being enforced. **CVE ID : CVE-2020-9915**		
N/A	16-Oct-20	5	A URL Unicode encoding issue was addressed with improved state management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A malicious attacker may be able to conceal the destination of a URL. **CVE ID : CVE-2020-9916**	N/A	O-APP-WATC-031120/923
Out-of-bounds Read	16-Oct-20	10	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. A remote attacker may be able to cause unexpected system termination or corrupt kernel memory. **CVE ID : CVE-2020-9918**	N/A	O-APP-WATC-031120/924
Out-of-bounds Write	22-Oct-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for	N/A	O-APP-WATC-031120/925

CVSS Scoring Scale	0-1	1-2	2-3	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 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9919**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Oct-20	6.4	A path handling issue was addressed with improved validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, watchOS 6.2.8. A malicious mail server may overwrite arbitrary mail files. **CVE ID : CVE-2020-9920**	N/A	O-APP-WATC-031120/926
N/A	16-Oct-20	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, watchOS 6.2.8. A malicious application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2020-9923**	N/A	O-APP-WATC-031120/927
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-20	4.3	A logic issue was addressed with improved state management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2020-9925**	N/A	O-APP-WATC-031120/928
Incorrect Authorizatio	16-Oct-20	4.3	An authorization issue was addressed with improved	N/A	O-APP-WATC-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			state management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8. A malicious application may be able to read sensitive location information. **CVE ID : CVE-2020-9933**		031120/929
Out-of-bounds Write	16-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9936**	N/A	O-APP-WATC-031120/930
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9937**	N/A	O-APP-WATC-031120/931
Out-of-bounds Read	22-Oct-20	6.8	An out-of-bounds read was addressed with improved input validation. This issue is	N/A	O-APP-WATC-031120/932

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9938**		
Improper Locking	16-Oct-20	4.6	This issue was addressed with improved checks. This issue is fixed in iOS 14.0 and iPadOS 14.0, watchOS 7.0. The screen lock may not engage after the specified time period. **CVE ID : CVE-2020-9946**	N/A	O-APP-WATC-031120/933
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-20	4.3	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 14.0 and iPadOS 14.0, tvOS 14.0, watchOS 7.0, Safari 14.0, iCloud for Windows 11.4, iCloud for Windows 7.21. Processing maliciously crafted web content may lead to a cross site scripting attack. **CVE ID : CVE-2020-9952**	N/A	O-APP-WATC-031120/934
N/A	16-Oct-20	4.3	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 14.0 and iPadOS 14.0, macOS Catalina 10.15.7, tvOS 14.0, watchOS 7.0. A malicious application may be able to access restricted files. **CVE ID : CVE-2020-9968**	N/A	O-APP-WATC-031120/935

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	16-Oct-20	4.3	A logic issue was addressed with improved state management. This issue is fixed in iOS 14.0 and iPadOS 14.0, tvOS 14.0, watchOS 7.0. A malicious application may be able to leak sensitive user information. **CVE ID : CVE-2020-9976**	N/A	O-APP-WATC-031120/936
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted font file may lead to arbitrary code execution. **CVE ID : CVE-2020-9980**	N/A	O-APP-WATC-031120/937
Out-of-bounds Read	22-Oct-20	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9984**	N/A	O-APP-WATC-031120/938
Buffer Copy without Checking Size of Input ('Classic Buffer	22-Oct-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, watchOS 6.2.8.	N/A	O-APP-WATC-031120/939

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
Overflow')			Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9985**		
N/A	22-Oct-20	5.8	A path handling issue was addressed with improved validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to overwrite arbitrary files. **CVE ID : CVE-2020-9994**	N/A	O-APP-WATC-031120/940
N/A	22-Oct-20	4.3	An information disclosure issue was addressed with improved state management. This issue is fixed in macOS Catalina 10.15.6, watchOS 6.2.8. A malicious application may disclose restricted memory. **CVE ID : CVE-2020-9997**	N/A	O-APP-WATC-031120/941
tvos					
Origin Validation Error	27-Oct-20	7.2	A logic issue was addressed with improved validation. This issue is fixed in iCloud for Windows 7.17, iTunes 12.10.4 for Windows, iCloud for Windows 10.9.2, tvOS 13.3.1, Safari 13.0.5, iOS 13.3.1 and iPadOS 13.3.1. A DOM object context may not have had a unique security origin. **CVE ID : CVE-2020-3864**	N/A	O-APP-TVOS-031120/942

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	27-Oct-20	9.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in watchOS 6.1.2, iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, macOS Catalina 10.15.3, Security Update 2020-001 Mojave, Security Update 2020-001 High Sierra. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-3880**	N/A	O-APP-TVOS-031120/943
N/A	22-Oct-20	2.1	An access issue was addressed with additional sandbox restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. A local user may be able to view sensitive user information. **CVE ID : CVE-2020-3918**	N/A	O-APP-TVOS-031120/944
N/A	22-Oct-20	2.1	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. A sandboxed process may be able to circumvent sandbox restrictions. **CVE ID : CVE-2020-9772**	N/A	O-APP-TVOS-031120/945
N/A	22-Oct-20	5	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. Some websites	N/A	O-APP-TVOS-031120/946

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may not have appeared in Safari Preferences. **CVE ID : CVE-2020-9787**		
N/A	22-Oct-20	4.6	A logic issue was addressed with improved validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5. An application may be able to gain elevated privileges. **CVE ID : CVE-2020-9854**	N/A	O-APP-TVOS-031120/947
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Oct-20	6.8	A command injection issue existed in Web Inspector. This issue was addressed with improved escaping. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Copying a URL from Web Inspector may lead to command injection. **CVE ID : CVE-2020-9862**	N/A	O-APP-TVOS-031120/948
Improper Initialization	22-Oct-20	9.3	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9863**	N/A	O-APP-TVOS-031120/949
Improper Restriction of	16-Oct-20	6.8	A memory corruption issue was addressed by removing the vulnerable code. This	N/A	O-APP-TVOS-031120/950

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. A malicious application may be able to break out of its sandbox. **CVE ID : CVE-2020-9865**		
Improper Certificate Validation	22-Oct-20	6.4	A certificate validation issue existed when processing administrator added certificates. This issue was addressed with improved certificate validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. An attacker may have been able to impersonate a trusted website using shared key material for an administrator added certificate. **CVE ID : CVE-2020-9868**	N/A	O-APP-TVOS-031120/951
Improper Input Validation	16-Oct-20	6.5	A logic issue was addressed with improved validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8. An attacker with memory write capability may be able to bypass pointer authentication codes and run arbitrary code. **CVE ID : CVE-2020-9870**	N/A	O-APP-TVOS-031120/952
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS	N/A	O-APP-TVOS-031120/953

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9871**		
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9872**	N/A	O-APP-TVOS-031120/954
Out-of-bounds Read	22-Oct-20	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9873**	N/A	O-APP-TVOS-031120/955
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking.	N/A	O-APP-TVOS-031120/956

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
			This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9874**		
Integer Overflow or Wraparound	22-Oct-20	6.8	An integer overflow was addressed through improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9875**	N/A	O-APP-TVOS-031120/957
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Opening a maliciously crafted PDF file may lead to an unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9876**	N/A	O-APP-TVOS-031120/958

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
Out-of-bounds Read	22-Oct-20	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9877**	N/A	O-APP-TVOS-031120/959
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Oct-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9878**	N/A	O-APP-TVOS-031120/960
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9879**	N/A	O-APP-TVOS-031120/961

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Oct-20	6.8	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9880**	N/A	O-APP-TVOS-031120/962
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Oct-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9883**	N/A	O-APP-TVOS-031120/963
Out-of-bounds Write	16-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9884**	N/A	O-APP-TVOS-031120/964
Insufficient Verification	16-Oct-20	4.3	An issue existed in the handling of iMessage	N/A	O-APP-TVOS-031120/965

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Data Authenticity			tapbacks. The issue was resolved with additional verification. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. A user that is removed from an iMessage group could rejoin the group. **CVE ID : CVE-2020-9885**		
Out-of-bounds Read	16-Oct-20	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9888**	N/A	O-APP-TVOS-031120/966
Out-of-bounds Write	16-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9889**	N/A	O-APP-TVOS-031120/967
Out-of-bounds Read	16-Oct-20	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted audio file may lead to	N/A	O-APP-TVOS-031120/968

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2020-9890**		
Out-of-bounds Read	16-Oct-20	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9891**	N/A	O-APP-TVOS-031120/969
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-Oct-20	9.3	Multiple memory corruption issues were addressed with improved state management. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. A malicious application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2020-9892**	N/A	O-APP-TVOS-031120/970
Use After Free	16-Oct-20	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9893**	N/A	O-APP-TVOS-031120/971
Out-of-	16-Oct-20	4.3	An out-of-bounds read was addressed with improved	N/A	O-APP-TVOS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9894**		031120/972
Use After Free	16-Oct-20	7.5	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9895**	N/A	O-APP-TVOS-031120/973
Improper Link Resolution Before File Access ('Link Following')	22-Oct-20	4.6	An issue existed within the path validation logic for symlinks. This issue was addressed with improved path sanitization. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2020-9900**	N/A	O-APP-TVOS-031120/974
Improper Link	22-Oct-20	4.6	An issue existed within the path validation logic for	N/A	O-APP-TVOS-031120/975

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
Resolution Before File Access ('Link Following')			symlinks. This issue was addressed with improved path sanitization. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2020-9901**		
Out-of-bounds Read	22-Oct-20	7.1	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. A malicious application may be able to determine kernel memory layout. **CVE ID : CVE-2020-9902**	N/A	O-APP-TVOS-031120/976
N/A	22-Oct-20	9.3	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9904**	N/A	O-APP-TVOS-031120/977
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Oct-20	5	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8. A remote attacker may be able to cause a denial of service. **CVE ID : CVE-2020-9905**	N/A	O-APP-TVOS-031120/978

CVSS Scoring Scale	0-1	1-2	2-3	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	16-Oct-20	9.3	A memory corruption issue was addressed by removing the vulnerable code. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9907**	N/A	O-APP-TVOS-031120/979
Out-of-bounds Read	16-Oct-20	4.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8. An attacker that has already achieved kernel code execution may be able to bypass kernel memory mitigations. **CVE ID : CVE-2020-9909**	N/A	O-APP-TVOS-031120/980
Improper Authenticati on	16-Oct-20	6.5	Multiple issues were addressed with improved logic. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A malicious attacker with arbitrary read and write capability may be able to bypass Pointer Authentication. **CVE ID : CVE-2020-9910**	N/A	O-APP-TVOS-031120/981
Improper Input Validation	16-Oct-20	5	An input validation issue existed in Bluetooth. This issue was addressed with improved input validation. This issue is fixed in iOS 13.6	N/A	O-APP-TVOS-031120/982

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
			and iPadOS 13.6, tvOS 13.4.8. An attacker in a privileged network position may be able to perform denial of service attack using malformed Bluetooth packets. **CVE ID : CVE-2020-9914**		
N/A	16-Oct-20	4.3	An access issue existed in Content Security Policy. This issue was addressed with improved access restrictions. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing maliciously crafted web content may prevent Content Security Policy from being enforced. **CVE ID : CVE-2020-9915**	N/A	O-APP-TVOS-031120/983
N/A	16-Oct-20	5	A URL Unicode encoding issue was addressed with improved state management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A malicious attacker may be able to conceal the destination of a URL. **CVE ID : CVE-2020-9916**	N/A	O-APP-TVOS-031120/984
Out-of-bounds Read	16-Oct-20	10	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina	N/A	O-APP-TVOS-031120/985

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
			10.15.6, tvOS 13.4.8, watchOS 6.2.8. A remote attacker may be able to cause unexpected system termination or corrupt kernel memory. **CVE ID : CVE-2020-9918**		
Out-of-bounds Write	22-Oct-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9919**	N/A	O-APP-TVOS-031120/986
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-20	4.3	A logic issue was addressed with improved state management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2020-9925**	N/A	O-APP-TVOS-031120/987
Incorrect Authorization	16-Oct-20	4.3	An authorization issue was addressed with improved state management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8. A malicious	N/A	O-APP-TVOS-031120/988

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			application may be able to read sensitive location information. **CVE ID : CVE-2020-9933**		
Out-of-bounds Write	16-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9936**	N/A	O-APP-TVOS-031120/989
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9937**	N/A	O-APP-TVOS-031120/990
Out-of-bounds Read	22-Oct-20	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows,	N/A	O-APP-TVOS-031120/991

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9938**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Oct-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9940**	N/A	O-APP-TVOS-031120/992
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-20	4.3	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 14.0 and iPadOS 14.0, tvOS 14.0, watchOS 7.0, Safari 14.0, iCloud for Windows 11.4, iCloud for Windows 7.21. Processing maliciously crafted web content may lead to a cross site scripting attack. **CVE ID : CVE-2020-9952**	N/A	O-APP-TVOS-031120/993
N/A	16-Oct-20	4.3	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 14.0 and iPadOS 14.0, macOS Catalina 10.15.7, tvOS 14.0, watchOS 7.0. A malicious application may be able to access restricted files. **CVE ID : CVE-2020-9968**	N/A	O-APP-TVOS-031120/994

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	16-Oct-20	4.3	A logic issue was addressed with improved state management. This issue is fixed in iOS 14.0 and iPadOS 14.0, tvOS 14.0, watchOS 7.0. A malicious application may be able to leak sensitive user information. **CVE ID : CVE-2020-9976**	N/A	O-APP-TVOS-031120/995
N/A	27-Oct-20	2.1	A trust issue was addressed by removing a legacy API. This issue is fixed in iOS 14.0 and iPadOS 14.0, tvOS 14.0. An attacker may be able to misuse a trust relationship to download malicious content. **CVE ID : CVE-2020-9979**	N/A	O-APP-TVOS-031120/996
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted font file may lead to arbitrary code execution. **CVE ID : CVE-2020-9980**	N/A	O-APP-TVOS-031120/997
Out-of-bounds Read	22-Oct-20	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to	N/A	O-APP-TVOS-031120/998

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2020-9984**		
N/A	22-Oct-20	5.8	A path handling issue was addressed with improved validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5, watchOS 6.2.5. A malicious application may be able to overwrite arbitrary files. **CVE ID : CVE-2020-9994**	N/A	O-APP-TVOS-031120/999
ipados					
Origin Validation Error	27-Oct-20	7.2	A logic issue was addressed with improved validation. This issue is fixed in iCloud for Windows 7.17, iTunes 12.10.4 for Windows, iCloud for Windows 10.9.2, tvOS 13.3.1, Safari 13.0.5, iOS 13.3.1 and iPadOS 13.3.1. A DOM object context may not have had a unique security origin. **CVE ID : CVE-2020-3864**	N/A	O-APP-IPAD-031120/1000
Out-of-bounds Read	27-Oct-20	9.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in watchOS 6.1.2, iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, macOS Catalina 10.15.3, Security Update 2020-001 Mojave, Security Update 2020-001 High Sierra. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-3880**	N/A	O-APP-IPAD-031120/1001

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	27-Oct-20	9.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Catalina 10.15.7, Security Update 2020-005 High Sierra, Security Update 2020-005 Mojave, iOS 14.0 and iPadOS 14.0. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9973**	N/A	O-APP-IPAD-031120/1002
N/A	27-Oct-20	2.1	A trust issue was addressed by removing a legacy API. This issue is fixed in iOS 14.0 and iPadOS 14.0, tvOS 14.0. An attacker may be able to misuse a trust relationship to download malicious content. **CVE ID : CVE-2020-9979**	N/A	O-APP-IPAD-031120/1003
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Oct-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, watchOS 6.2.8. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9985**	N/A	O-APP-IPAD-031120/1004
N/A	22-Oct-20	5.8	A path handling issue was addressed with improved validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, macOS Catalina 10.15.5, tvOS	N/A	O-APP-IPAD-031120/1005

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			13.4.5, watchOS 6.2.5. A malicious application may be able to overwrite arbitrary files. **CVE ID : CVE-2020-9994**		
ipad_os					
N/A	22-Oct-20	2.1	An access issue was addressed with additional sandbox restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. A local user may be able to view sensitive user information. **CVE ID : CVE-2020-3918**	N/A	O-APP-IPAD-031120/1006
N/A	22-Oct-20	2.1	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. A sandboxed process may be able to circumvent sandbox restrictions. **CVE ID : CVE-2020-9772**	N/A	O-APP-IPAD-031120/1007
N/A	22-Oct-20	5	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. Some websites may not have appeared in Safari Preferences. **CVE ID : CVE-2020-9787**	N/A	O-APP-IPAD-031120/1008
N/A	22-Oct-20	4.6	A logic issue was addressed with improved validation. This issue is fixed in iOS 13.5	N/A	O-APP-IPAD-031120/1009

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and iPadOS 13.5, macOS Catalina 10.15.5, tvOS 13.4.5. An application may be able to gain elevated privileges. **CVE ID : CVE-2020-9854**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Oct-20	6.8	A command injection issue existed in Web Inspector. This issue was addressed with improved escaping. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Copying a URL from Web Inspector may lead to command injection. **CVE ID : CVE-2020-9862**	N/A	O-APP-IPAD-031120/1010
Improper Initialization	22-Oct-20	9.3	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9863**	N/A	O-APP-IPAD-031120/1011
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Oct-20	6.8	A memory corruption issue was addressed by removing the vulnerable code. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. A malicious application may be able to break out of its sandbox.	N/A	O-APP-IPAD-031120/1012

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9865		
Improper Certificate Validation	22-Oct-20	6.4	A certificate validation issue existed when processing administrator added certificates. This issue was addressed with improved certificate validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. An attacker may have been able to impersonate a trusted website using shared key material for an administrator added certificate. **CVE ID : CVE-2020-9868**	N/A	O-APP-IPAD-031120/1013
Improper Input Validation	16-Oct-20	6.5	A logic issue was addressed with improved validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8. An attacker with memory write capability may be able to bypass pointer authentication codes and run arbitrary code. **CVE ID : CVE-2020-9870**	N/A	O-APP-IPAD-031120/1014
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code	N/A	O-APP-IPAD-031120/1015

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
			execution. **CVE ID : CVE-2020-9871**		
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9872**	N/A	O-APP-IPAD-031120/1016
Out-of-bounds Read	22-Oct-20	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9873**	N/A	O-APP-IPAD-031120/1017
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a	N/A	O-APP-IPAD-031120/1018

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9874**		
Integer Overflow or Wraparound	22-Oct-20	6.8	An integer overflow was addressed through improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9875**	N/A	O-APP-IPAD-031120/1019
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Opening a maliciously crafted PDF file may lead to an unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9876**	N/A	O-APP-IPAD-031120/1020
Out-of-bounds Read	22-Oct-20	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows,	N/A	O-APP-IPAD-031120/1021

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9877**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-Oct-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9878**	N/A	O-APP-IPAD-031120/1022
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9879**	N/A	O-APP-IPAD-031120/1023
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Oct-20	6.8	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously	N/A	O-APP-IPAD-031120/1024

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9880**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Oct-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, watchOS 6.2.8. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9881**	N/A	O-APP-IPAD-031120/1025
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Oct-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, watchOS 6.2.8. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9882**	N/A	O-APP-IPAD-031120/1026
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Oct-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a	N/A	O-APP-IPAD-031120/1027

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9883**		
Out-of-bounds Write	16-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9884**	N/A	O-APP-IPAD-031120/1028
Insufficient Verification of Data Authenticity	16-Oct-20	4.3	An issue existed in the handling of iMessage tapbacks. The issue was resolved with additional verification. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. A user that is removed from an iMessage group could rejoin the group. **CVE ID : CVE-2020-9885**	N/A	O-APP-IPAD-031120/1029
Out-of-bounds Read	16-Oct-20	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9888**	N/A	O-APP-IPAD-031120/1030
Out-of-bounds	16-Oct-20	6.8	An out-of-bounds write issue was addressed with	N/A	O-APP-IPAD-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9889**		031120/1031
Out-of-bounds Read	16-Oct-20	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9890**	N/A	O-APP-IPAD-031120/1032
Out-of-bounds Read	16-Oct-20	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted audio file may lead to arbitrary code execution. **CVE ID : CVE-2020-9891**	N/A	O-APP-IPAD-031120/1033
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-Oct-20	9.3	Multiple memory corruption issues were addressed with improved state management. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. A malicious application may be able to execute arbitrary code with system privileges.	N/A	O-APP-IPAD-031120/1034

CVSS Scoring Scale	0-1	1-2	2-3	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-2020-9892		
Use After Free	16-Oct-20	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9893**	N/A	O-APP-IPAD-031120/1035
Out-of-bounds Read	16-Oct-20	4.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9894**	N/A	O-APP-IPAD-031120/1036
Use After Free	16-Oct-20	7.5	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A remote attacker may be able to cause unexpected	N/A	O-APP-IPAD-031120/1037

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			application termination or arbitrary code execution. **CVE ID : CVE-2020-9895**		
N/A	22-Oct-20	7.5	This issue was addressed with improved entitlements. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6. A sandboxed process may be able to circumvent sandbox restrictions. **CVE ID : CVE-2020-9898**	N/A	O-APP-IPAD-031120/1038
Improper Link Resolution Before File Access ('Link Following')	22-Oct-20	4.6	An issue existed within the path validation logic for symlinks. This issue was addressed with improved path sanitization. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2020-9900**	N/A	O-APP-IPAD-031120/1039
Improper Link Resolution Before File Access ('Link Following')	22-Oct-20	4.6	An issue existed within the path validation logic for symlinks. This issue was addressed with improved path sanitization. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2020-9901**	N/A	O-APP-IPAD-031120/1040
Out-of-bounds Read	22-Oct-20	7.1	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6,	N/A	O-APP-IPAD-031120/1041

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			tvOS 13.4.8, watchOS 6.2.8. A malicious application may be able to determine kernel memory layout. **CVE ID : CVE-2020-9902**		
Origin Validation Error	16-Oct-20	5	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.6 and iPadOS 13.6, Safari 13.1.2. A malicious attacker may cause Safari to suggest a password for the wrong domain. **CVE ID : CVE-2020-9903**	N/A	O-APP-IPAD-031120/1042
N/A	22-Oct-20	9.3	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9904**	N/A	O-APP-IPAD-031120/1043
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Oct-20	5	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8. A remote attacker may be able to cause a denial of service. **CVE ID : CVE-2020-9905**	N/A	O-APP-IPAD-031120/1044
Improper Input Validation	22-Oct-20	9.4	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS	N/A	O-APP-IPAD-031120/1045

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Catalina 10.15.6, watchOS 6.2.8. A remote attacker may be able to cause unexpected system termination or corrupt kernel memory. **CVE ID : CVE-2020-9906**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Oct-20	9.3	A memory corruption issue was addressed by removing the vulnerable code. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8. An application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9907**	N/A	O-APP-IPAD-031120/1046
Out-of-bounds Read	16-Oct-20	4.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8. An attacker that has already achieved kernel code execution may be able to bypass kernel memory mitigations. **CVE ID : CVE-2020-9909**	N/A	O-APP-IPAD-031120/1047
Improper Authenticati on	16-Oct-20	6.5	Multiple issues were addressed with improved logic. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A malicious attacker with arbitrary read and write capability may be able to bypass Pointer Authentication.	N/A	O-APP-IPAD-031120/1048

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9910		
N/A	16-Oct-20	5	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.6 and iPadOS 13.6, Safari 13.1.2. An issue in Safari Reader mode may allow a remote attacker to bypass the Same Origin Policy. **CVE ID : CVE-2020-9911**	N/A	O-APP-IPAD-031120/1049
Improper Input Validation	16-Oct-20	5	An input validation issue existed in Bluetooth. This issue was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8. An attacker in a privileged network position may be able to perform denial of service attack using malformed Bluetooth packets. **CVE ID : CVE-2020-9914**	N/A	O-APP-IPAD-031120/1050
N/A	16-Oct-20	4.3	An access issue existed in Content Security Policy. This issue was addressed with improved access restrictions. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing maliciously crafted web content may prevent Content Security Policy from being enforced. **CVE ID : CVE-2020-9915**	N/A	O-APP-IPAD-031120/1051
N/A	16-Oct-20	5	A URL Unicode encoding issue was addressed with	N/A	O-APP-IPAD-031120/1052

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improved state management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A malicious attacker may be able to conceal the destination of a URL. **CVE ID : CVE-2020-9916**		
N/A	16-Oct-20	5	This issue was addressed with improved checks. This issue is fixed in iOS 13.6 and iPadOS 13.6. A remote attacker may be able to cause a denial of service. **CVE ID : CVE-2020-9917**	N/A	O-APP-IPAD-031120/1053
Out-of-bounds Read	16-Oct-20	10	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. A remote attacker may be able to cause unexpected system termination or corrupt kernel memory. **CVE ID : CVE-2020-9918**	N/A	O-APP-IPAD-031120/1054
Out-of-bounds Write	22-Oct-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image	N/A	O-APP-IPAD-031120/1055

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may lead to arbitrary code execution. **CVE ID : CVE-2020-9919**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Oct-20	6.4	A path handling issue was addressed with improved validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, watchOS 6.2.8. A malicious mail server may overwrite arbitrary mail files. **CVE ID : CVE-2020-9920**	N/A	O-APP-IPAD-031120/1056
N/A	16-Oct-20	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, watchOS 6.2.8. A malicious application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2020-9923**	N/A	O-APP-IPAD-031120/1057
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-20	4.3	A logic issue was addressed with improved state management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing maliciously crafted web content may lead to universal cross site scripting. **CVE ID : CVE-2020-9925**	N/A	O-APP-IPAD-031120/1058
Improper Input Validation	16-Oct-20	5	A denial of service issue was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS	N/A	O-APP-IPAD-031120/1059

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			13.6. A remote attacker may cause an unexpected application termination. **CVE ID : CVE-2020-9931**		
Incorrect Authorization	16-Oct-20	4.3	An authorization issue was addressed with improved state management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8. A malicious application may be able to read sensitive location information. **CVE ID : CVE-2020-9933**	N/A	O-APP-IPAD-031120/1060
N/A	16-Oct-20	2.1	An issue existed in the handling of environment variables. This issue was addressed with improved validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6. A local user may be able to view sensitive user information. **CVE ID : CVE-2020-9934**	N/A	O-APP-IPAD-031120/1061
Out-of-bounds Write	16-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9936**	N/A	O-APP-IPAD-031120/1062

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9937**	N/A	O-APP-IPAD-031120/1063
Out-of-bounds Read	22-Oct-20	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9938**	N/A	O-APP-IPAD-031120/1064
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Oct-20	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-9940**	N/A	O-APP-IPAD-031120/1065

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Locking	16-Oct-20	4.6	This issue was addressed with improved checks. This issue is fixed in iOS 14.0 and iPadOS 14.0, watchOS 7.0. The screen lock may not engage after the specified time period. **CVE ID : CVE-2020-9946**	N/A	O-APP-IPAD-031120/1066
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-20	4.3	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 14.0 and iPadOS 14.0, tvOS 14.0, watchOS 7.0, Safari 14.0, iCloud for Windows 11.4, iCloud for Windows 7.21. Processing maliciously crafted web content may lead to a cross site scripting attack. **CVE ID : CVE-2020-9952**	N/A	O-APP-IPAD-031120/1067
Out-of-bounds Write	16-Oct-20	9.3	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 14.0 and iPadOS 14.0. An application may be able to cause unexpected system termination or write kernel memory. **CVE ID : CVE-2020-9958**	N/A	O-APP-IPAD-031120/1068
Improper Locking	16-Oct-20	2.1	A lock screen issue allowed access to messages on a locked device. This issue was addressed with improved state management. This issue is fixed in iOS 14.0 and iPadOS 14.0. A person with physical access to an iOS device may be able to view	N/A	O-APP-IPAD-031120/1069

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			notification contents from the lockscreen. **CVE ID : CVE-2020-9959**		
Improper Initialization	16-Oct-20	4.9	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 14.0 and iPadOS 14.0. A local user may be able to read kernel memory. **CVE ID : CVE-2020-9964**	N/A	O-APP-IPAD-031120/1070
N/A	16-Oct-20	4.3	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 14.0 and iPadOS 14.0, macOS Catalina 10.15.7, tvOS 14.0, watchOS 7.0. A malicious application may be able to access restricted files. **CVE ID : CVE-2020-9968**	N/A	O-APP-IPAD-031120/1071
Information Exposure	16-Oct-20	4.3	A logic issue was addressed with improved state management. This issue is fixed in iOS 14.0 and iPadOS 14.0, tvOS 14.0, watchOS 7.0. A malicious application may be able to leak sensitive user information. **CVE ID : CVE-2020-9976**	N/A	O-APP-IPAD-031120/1072
Out-of-bounds Write	22-Oct-20	6.8	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8. Processing a maliciously crafted font file may lead to arbitrary code	N/A	O-APP-IPAD-031120/1073

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2020-9980**		
Out-of-bounds Read	22-Oct-20	6.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, macOS Catalina 10.15.6, tvOS 13.4.8, watchOS 6.2.8, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2020-9984**	N/A	O-APP-IPAD-031120/1074
N/A	16-Oct-20	9.3	This issue was addressed by encrypting communications over the network to devices running iOS 14, iPadOS 14, tvOS 14, and watchOS 7. This issue is fixed in iOS 14.0 and iPadOS 14.0, Xcode 12.0. An attacker in a privileged network position may be able to execute arbitrary code on a paired device during a debug session over the network. **CVE ID : CVE-2020-9992**	N/A	O-APP-IPAD-031120/1075
Belkin					
linksys_wrt_160nl_firmware					
Out-of-bounds Write	23-Oct-20	6.5	** UNSUPPORTED WHEN ASSIGNED ** Belkin LINKSYS WRT160NL 1.0.04.002_US_20130619 devices have a stack-based buffer overflow vulnerability because of sprintf in create_dir in mini_httpd. Successful exploitation leads	N/A	O-BEL-LINK-031120/1076

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to arbitrary code execution. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2020-26561**		
Canonical					
ubuntu_linux					
Insufficiently Protected Credentials	16-Oct-20	4.3	In containerd (an industry-standard container runtime) before version 1.2.14 there is a credential leaking vulnerability. If a container image manifest in the OCI Image format or Docker Image V2 Schema 2 format includes a URL for the location of a specific image layer (otherwise known as a "foreign layer"), the default containerd resolver will follow that URL to attempt to download it. In v1.2.x but not 1.3.0 or later, the default containerd resolver will provide its authentication credentials if the server where the URL is located presents an HTTP 401 status code along with registry-specific HTTP headers. If an attacker publishes a public image with a manifest that directs one of the layers to be fetched from a web server they control and they trick a user or system into pulling the image, they can obtain the credentials used for pulling that image. In some cases,	https://github.com/containerd/containerd/security/advisories/GHSA-742w-89gc-8m9c	O-CAN-UBUN-031120/1077

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			this may be the user's username and password for the registry. In other cases, this may be the credentials attached to the cloud virtual instance which can grant access to other cloud resources in the account. The default containerd resolver is used by the cri-containerd plugin (which can be used by Kubernetes), the ctr development tool, and other client programs that have explicitly linked against it. This vulnerability has been fixed in containerd 1.2.14. containerd 1.3 and later are not affected. If you are using containerd 1.3 or later, you are not affected. If you are using cri-containerd in the 1.2 series or prior, you should ensure you only pull images from trusted sources. Other container runtimes built on top of containerd but not using the default resolver (such as Docker) are not affected. **CVE ID : CVE-2020-15157**		
Cisco					
firepower_extensible_operating_system					
Improper Neutralization of Special Elements used in an OS Command ('OS	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to	N/A	O-CIS-FIRE-031120/1078

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3457**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3459**	N/A	O-CIS-FIRE-031120/1079
N/A	21-Oct-20	7.2	A vulnerability in the secure boot process of Cisco FXOS Software could allow an authenticated, local attacker to bypass the secure boot mechanisms. The vulnerability is due to	N/A	O-CIS-FIRE-031120/1080

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			insufficient protections of the secure boot process. An attacker could exploit this vulnerability by injecting code into a specific file that is then referenced during the device boot process. A successful exploit could allow the attacker to break the chain of trust and inject code into the boot process of the device which would be executed at each boot and maintain persistence across reboots. **CVE ID : CVE-2020-3455**		
Cross-Site Request Forgery (CSRF)	21-Oct-20	6.8	A vulnerability in the Cisco Firepower Chassis Manager (FCM) of Cisco FXOS Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of an affected device. The vulnerability is due to insufficient CSRF protections for the FCM interface. An attacker could exploit this vulnerability by persuading a targeted user to click a malicious link. A successful exploit could allow the attacker to send arbitrary requests that could take unauthorized actions on behalf of the targeted user. **CVE ID : CVE-2020-3456**	N/A	O-CIS-FIRE-031120/1081
firepower_threat_defense					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3457**	N/A	O-CIS-FIRE-031120/1082
Incorrect Authorization	21-Oct-20	5.8	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass a configured access rule and access parts of the WebVPN portal that are supposed to be blocked. The vulnerability is due to insufficient validation of URLs when portal access rules are configured. An attacker could exploit this vulnerability by accessing certain URLs on the affected device. **CVE ID : CVE-2020-3578**	N/A	O-CIS-FIRE-031120/1083

CVSS Scoring Scale	0-1	1-2	2-3	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')	21-Oct-20	2.6	Multiple vulnerabilities in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the web services interface of an affected device. The vulnerabilities are due to insufficient validation of user-supplied input by the web services interface of an affected device. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive, browser-based information. Note: These vulnerabilities affect only specific AnyConnect and WebVPN configurations. For more information, see the Vulnerable Products section. **CVE ID : CVE-2020-3580**	N/A	O-CIS-FIRE-031120/1084
Improper Neutralization of Input During Web Page Generation	21-Oct-20	2.6	Multiple vulnerabilities in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software	N/A	O-CIS-FIRE-031120/1085

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the web services interface of an affected device. The vulnerabilities are due to insufficient validation of user-supplied input by the web services interface of an affected device. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive, browser-based information. Note: These vulnerabilities affect only specific AnyConnect and WebVPN configurations. For more information, see the Vulnerable Products section. **CVE ID : CVE-2020-3581**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Oct-20	2.6	Multiple vulnerabilities in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the web services interface of an	N/A	O-CIS-FIRE-031120/1086

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device. The vulnerabilities are due to insufficient validation of user-supplied input by the web services interface of an affected device. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive, browser-based information. Note: These vulnerabilities affect only specific AnyConnect and WebVPN configurations. For more information, see the Vulnerable Products section. **CVE ID : CVE-2020-3582**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Oct-20	4.3	Multiple vulnerabilities in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the web services interface of an affected device. The vulnerabilities are due to insufficient validation of user-supplied input by the web services interface of an affected device. An attacker	N/A	O-CIS-FIRE-031120/1087

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive, browser-based information. Note: These vulnerabilities affect only specific AnyConnect and WebVPN configurations. For more information, see the Vulnerable Products section. **CVE ID : CVE-2020-3583**		
Information Exposure Through Discrepancy	21-Oct-20	4.3	A vulnerability in the TLS handler of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 1000 Series firewalls could allow an unauthenticated, remote attacker to gain access to sensitive information. The vulnerability is due to improper implementation of countermeasures against the Bleichenbacher attack for cipher suites that rely on RSA for key exchange. An attacker could exploit this vulnerability by sending crafted TLS messages to the device, which would act as an oracle and allow the attacker to carry out a chosen-ciphertext attack. A	N/A	O-CIS-FIRE-031120/1088

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to perform cryptanalytic operations that may allow decryption of previously captured TLS sessions to the affected device. To exploit this vulnerability, an attacker must be able to perform both of the following actions: Capture TLS traffic that is in transit between clients and the affected device Actively establish a considerable number of TLS connections to the affected device **CVE ID : CVE-2020-3585**		
adaptive_security_appliance_software					
Incorrect Authorizatio n	21-Oct-20	5.8	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass a configured access rule and access parts of the WebVPN portal that are supposed to be blocked. The vulnerability is due to insufficient validation of URLs when portal access rules are configured. An attacker could exploit this vulnerability by accessing certain URLs on the affected device. **CVE ID : CVE-2020-3578**	N/A	O-CIS-ADAP-031120/1089
Improper Neutralizatio	21-Oct-20	2.6	Multiple vulnerabilities in the web services interface of	N/A	O-CIS-ADAP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the web services interface of an affected device. The vulnerabilities are due to insufficient validation of user-supplied input by the web services interface of an affected device. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive, browser-based information. Note: These vulnerabilities affect only specific AnyConnect and WebVPN configurations. For more information, see the Vulnerable Products section. **CVE ID : CVE-2020-3580**		031120/1090
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site	21-Oct-20	2.6	Multiple vulnerabilities in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote	N/A	O-CIS-ADAP-031120/1091

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			attacker to conduct cross-site scripting (XSS) attacks against a user of the web services interface of an affected device. The vulnerabilities are due to insufficient validation of user-supplied input by the web services interface of an affected device. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive, browser-based information. Note: These vulnerabilities affect only specific AnyConnect and WebVPN configurations. For more information, see the Vulnerable Products section. **CVE ID : CVE-2020-3581**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Oct-20	2.6	Multiple vulnerabilities in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the web services interface of an affected device. The vulnerabilities are due to	N/A	O-CIS-ADAP-031120/1092

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			insufficient validation of user-supplied input by the web services interface of an affected device. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive, browser-based information. Note: These vulnerabilities affect only specific AnyConnect and WebVPN configurations. For more information, see the Vulnerable Products section. **CVE ID : CVE-2020-3582**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Oct-20	4.3	Multiple vulnerabilities in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the web services interface of an affected device. The vulnerabilities are due to insufficient validation of user-supplied input by the web services interface of an affected device. An attacker could exploit these vulnerabilities by persuading	N/A	O-CIS-ADAP-031120/1093

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive, browser-based information. Note: These vulnerabilities affect only specific AnyConnect and WebVPN configurations. For more information, see the Vulnerable Products section. **CVE ID : CVE-2020-3583**		
Information Exposure Through Discrepancy	21-Oct-20	4.3	A vulnerability in the TLS handler of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 1000 Series firewalls could allow an unauthenticated, remote attacker to gain access to sensitive information. The vulnerability is due to improper implementation of countermeasures against the Bleichenbacher attack for cipher suites that rely on RSA for key exchange. An attacker could exploit this vulnerability by sending crafted TLS messages to the device, which would act as an oracle and allow the attacker to carry out a chosen-ciphertext attack. A successful exploit could allow the attacker to perform	N/A	O-CIS-ADAP-031120/1094

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cryptanalytic operations that may allow decryption of previously captured TLS sessions to the affected device. To exploit this vulnerability, an attacker must be able to perform both of the following actions: Capture TLS traffic that is in transit between clients and the affected device Actively establish a considerable number of TLS connections to the affected device **CVE ID : CVE-2020-3585**		
Debian					
debian_linux					
N/A	21-Oct-20	5.8	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Java SE: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. 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. 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	https://security.netapp.com/advisory/ntap-20201023-0004/	O-DEB-DEBI-031120/1095

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 4.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N). **CVE ID : CVE-2020-14792**		
N/A	21-Oct-20	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported versions that are affected are Java SE: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. 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	https://security.netapp.com/advisory/ntap-20201023-0004/	O-DEB-DEBI-031120/1096

CVSS Scoring Scale	0-1	1-2	2-3	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 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-2020-14779**		
N/A	21-Oct-20	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: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. 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. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed	https://security.netapp.com/advisory/ntap-20201023-0004/	O-DEB-DEBI-031120/1097

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2020-14782**		
N/A	22-Oct-20	7.5	Mozilla developers and community members reported memory safety bugs present in Firefox 81 and Firefox ESR 78.3. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox ESR < 78.4, Firefox < 82, and Thunderbird < 78.4. **CVE ID : CVE-2020-15683**	N/A	O-DEB-DEBI-031120/1098
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-Oct-20	5	receive.c in fastd before v21 allows denial of service (assertion failure) when receiving packets with an invalid type code. **CVE ID : CVE-2020-27638**	N/A	O-DEB-DEBI-031120/1099
Fedoraproject					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
fedora					
N/A	21-Oct-20	4.3	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported versions that are affected are Java SE: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. 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-2020-14779**	https://security.netapp.com/advisory/ntap-20201023-0004/	O-FED-FEDO-031120/1100
Insufficient	19-Oct-20	5	An issue was discovered in	N/A	O-FED-FEDO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Session Expiration			the yh_create_session() function of yubihsm-shell through 2.0.2. The function does not explicitly check the returned session id from the device. An invalid session id would lead to out-of-bounds read and write operations in the session array. This could be used by an attacker to cause a denial of service attack. **CVE ID : CVE-2020-24387**		031120/1101
Improper Input Validation	19-Oct-20	5	An issue was discovered in the _send_secure_msg() function of yubihsm-shell through 2.0.2. The function does not validate the embedded length field of a message received from the device. This could lead to an oversized memcpy() call that will crash the running process. This could be used by an attacker to cause a denial of service. **CVE ID : CVE-2020-24388**	N/A	O-FED-FEDO-031120/1102
Fortinet					
fortios					
Cleartext Storage of Sensitive Information	21-Oct-20	4	A cleartext storage of sensitive information vulnerability in FortiOS command line interface in versions 6.2.4 and below may allow an authenticated attacker to obtain sensitive information such as users passwords by connecting to FortiGate CLI and executing	https://www.fortiguard.com/psirt/FG-IR-20-009	O-FOR-FORT-031120/1103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the "diag sys ha checksum show" command. **CVE ID : CVE-2020-6648**		
free					
freebox_v5_firmware					
Authentication Bypass by Spoofing	19-Oct-20	4.3	A DNS rebinding vulnerability in the UPnP MediaServer implementation in Freebox Server before 4.2.3. **CVE ID : CVE-2020-24375**	https://dev.freebox.fr/blog/?p=10222	O-FRE-FREE-031120/1104
GE					
s2020_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-20	4.3	The affected Reason S20 Ethernet Switch is vulnerable to cross-site scripting (XSS), which may allow attackers to trick users into following a link or navigating to a page that posts a malicious JavaScript statement to the vulnerable site, causing the malicious JavaScript to be rendered by the site and executed by the victim client. **CVE ID : CVE-2020-16246**	N/A	O-GE-S202-031120/1105
s2024_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-20	4.3	The affected Reason S20 Ethernet Switch is vulnerable to cross-site scripting (XSS), which may allow attackers to trick users into following a link or navigating to a page that posts a malicious JavaScript statement to the vulnerable site, causing the malicious JavaScript to be rendered by the site and	N/A	O-GE-S202-031120/1106

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			executed by the victim client. **CVE ID : CVE-2020-16246**		
Huawei					
e6878-370_firmware					
N/A	19-Oct-20	2.7	E6878-370 versions 10.0.3.1(H557SP27C233),10.0.3.1(H563SP21C233) and E6878-870 versions 10.0.3.1(H557SP27C233),10.0.3.1(H563SP11C233) have a denial of service vulnerability. The system does not properly check some events, an attacker could launch the events continually, successful exploit could cause reboot of the process. **CVE ID : CVE-2020-9111**	N/A	O-HUA-E687-031120/1107
e6878-870_firmware					
N/A	19-Oct-20	2.7	E6878-370 versions 10.0.3.1(H557SP27C233),10.0.3.1(H563SP21C233) and E6878-870 versions 10.0.3.1(H557SP27C233),10.0.3.1(H563SP11C233) have a denial of service vulnerability. The system does not properly check some events, an attacker could launch the events continually, successful exploit could cause reboot of the process. **CVE ID : CVE-2020-9111**	N/A	O-HUA-E687-031120/1108
taurus-an00b_firmware					
Improper Privilege Management	19-Oct-20	4.6	Taurus-AN00B versions earlier than 10.1.0.156(C00E155R7P2) have a privilege elevation	N/A	O-HUA-TAUR-031120/1109

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. Due to lack of privilege restrictions on some of the business functions of the device. An attacker could exploit this vulnerability to access the protecting information, resulting in the elevation of the privilege. **CVE ID : CVE-2020-9112**		
p30_firmware					
Use After Free	19-Oct-20	6.8	HUAWEI Mate 30 versions earlier than 10.1.0.150(C00E136R5P3) and HUAWEI P30 version earlier than 10.1.0.160(C00E160R2P11) 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 common privilege, successful exploit could cause code execution. **CVE ID : CVE-2020-9263**	N/A	O-HUA-P30_-031120/1110
mate_20_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-Oct-20	2.1	HUAWEI Mate 20 versions earlier than 10.1.0.163(C00E160R3P8) have a JavaScript injection vulnerability. A module does not verify a specific input. This could allow attackers to bypass filter mechanism to launch JavaScript injection. This could compromise	N/A	O-HUA-MATE-031120/1111

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			normal service of the affected module. **CVE ID : CVE-2020-9092**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-20	5.4	HUAWEI Mate 20 versions earlier than 10.0.0.188(C00E74R3P8) have a buffer overflow vulnerability in the Bluetooth module. Due to insufficient input validation, an unauthenticated attacker may craft Bluetooth messages after successful paring, causing buffer overflow. Successful exploit may cause code execution. **CVE ID : CVE-2020-9113**	N/A	O-HUA-MATE-031120/1112
mate_30_firmware					
Use After Free	19-Oct-20	6.8	HUAWEI Mate 30 versions earlier than 10.1.0.150(C00E136R5P3) and HUAWEI P30 version earlier than 10.1.0.160(C00E160R2P11) 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 common privilege, successful exploit could cause code execution. **CVE ID : CVE-2020-9263**	N/A	O-HUA-MATE-031120/1113
Illumos					
illumos					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	26-Oct-20	7.5	An issue was discovered in illumos before 2020-10-22, as used in OmniOS before r151030by, r151032ay, and r151034y and SmartOS before 20201022. There is a buffer overflow in parse_user_name in lib/libpam/pam_framework.c . **CVE ID : CVE-2020-27678**	N/A	O-ILL-ILLU-031120/1114
Joyent					
smartos					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	26-Oct-20	7.5	An issue was discovered in illumos before 2020-10-22, as used in OmniOS before r151030by, r151032ay, and r151034y and SmartOS before 20201022. There is a buffer overflow in parse_user_name in lib/libpam/pam_framework.c . **CVE ID : CVE-2020-27678**	N/A	O-JOY-SMAR-031120/1115
Juniper					
junos					
Improper Input Validation	16-Oct-20	5.8	The DHCPv6 Relay-Agent service, part of the Juniper Enhanced jdhcpd daemon shipped with Juniper Networks Junos OS has an Improper Input Validation vulnerability which will result in a Denial of Service (DoS) condition when a DHCPv6 client sends a specific DHPCv6 message allowing an attacker to potentially perform a Remote	https://kb.juniper.net/JSA11049	O-JUN-JUNO-031120/1116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Code Execution (RCE) attack on the target device. Continuous receipt of the specific DHCPv6 client message will result in an extended Denial of Service (DoS) condition. If adjacent devices are also configured to relay DHCP packets, and are not affected by this issue and simply transparently forward unprocessed client DHCPv6 messages, then the attack vector can be a Network-based attack, instead of an Adjacent-device attack. No other DHCP services are affected. Receipt of the packet without configuration of the DHCPv6 Relay-Agent service, will not result in exploitability of this issue. This issue affects Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S15; 12.3X48 versions prior to 12.3X48-D95; 14.1X53 versions prior to 14.1X53-D53; 15.1 versions prior to 15.1R7-S6; 15.1X49 versions prior to 15.1X49-D200; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2; 17.2 versions prior to 17.2R3-S3; 17.2X75 versions prior to 17.2X75-D44; 17.3 versions prior to 17.3R3-S7; 17.4		

CVSS Scoring Scale	0-1	1-2	2-3	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 prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R2-S6, 18.2R3-S2; 18.2X75 versions prior to 18.2X75-D12, 18.2X75-D33, 18.2X75-D435, 18.2X75-D60; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R3; 19.1 versions prior to 19.1R1-S4, 19.1R2; 19.2 versions prior to 19.2R1-S3, 19.2R2; 19.3 versions prior to 19.3R2. **CVE ID : CVE-2020-1656**		
N/A	16-Oct-20	5	On SRX Series devices, a vulnerability in the key-management-daemon (kmd) daemon of Juniper Networks Junos OS allows an attacker to spoof packets targeted to IPSec peers before a security association (SA) is established thereby causing a failure to set up the IPSec channel. Sustained receipt of these spoofed packets can cause a sustained Denial of Service (DoS) condition. This issue affects IPv4 and IPv6 implementations. This issue affects Juniper Networks Junos OS on SRX Series: 12.3X48 versions prior to 12.3X48-D90; 15.1X49 versions prior to 15.1X49-D190; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S9;	https://kb.juniper.net/JSA11050	O-JUN-JUNO-031120/1117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.2 versions prior to 18.2R3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R1-S6, 18.4R2-S3, 18.4R3; 19.1 versions prior to 19.1R1-S4, 19.1R2. This issue does not affect 12.3 or 15.1 releases which are non-SRX Series releases. **CVE ID : CVE-2020-1657**		
N/A	16-Oct-20	6.8	When DNS filtering is enabled on Juniper Networks Junos MX Series with one of the following cards MS-PIC, MS-MIC or MS-MPC, an incoming stream of packets processed by the Multiservices PIC Management Daemon (mspmand) process, responsible for managing "URL Filtering service", may crash, causing the Services PIC to restart. While the Services PIC is restarting, all PIC services including DNS filtering service (DNS sink holing) will be bypassed until the Services PIC completes its boot process. This vulnerability might allow an attacker to cause an extended Denial of Service (DoS) attack against the device and to cause clients to be vulnerable to DNS based attacks by malicious DNS servers when they send DNS requests through the device. As a result, devices which were once protected by the DNS	https://kb.juniper.net/JSA11054	O-JUN-JUNO-031120/1118

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Filtering service are no longer protected and at risk of exploitation. This issue affects Juniper Networks Junos OS: 17.3 versions prior to 17.3R3-S8; 18.3 versions prior to 18.3R3-S1; 18.4 versions prior to 18.4R3; 19.1 versions prior to 19.1R3; 19.2 versions prior to 19.2R2; 19.3 versions prior to 19.3R3. This issue does not affect Juniper Networks Junos OS 17.4, 18.1, and 18.2. **CVE ID : CVE-2020-1660**		
N/A	16-Oct-20	4.3	On Juniper Networks Junos OS devices configured as a DHCP forwarder, the Juniper Networks Dynamic Host Configuration Protocol Daemon (jdhcp) process might crash when receiving a malformed DHCP packet. This issue only affects devices configured as DHCP forwarder with forward-only option, that forward specified DHCP client packets, without creating a new subscriber session. The jdhcpd daemon automatically restarts without intervention, but continuous receipt of the malformed DHCP packet will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. This issue can be triggered only by DHCPv4, it cannot be triggered by DHCPv6. This issue affects Juniper	https://kb.juniper.net/JSA11056	O-JUN-JUNO-031120/1119

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS: 12.3 versions prior to 12.3R12-S16; 12.3X48 versions prior to 12.3X48-D105 on SRX Series; 14.1X53 versions prior to 14.1X53-D60 on EX and QFX Series; 15.1 versions prior to 15.1R7-S7; 15.1X49 versions prior to 15.1X49-D221, 15.1X49-D230 on SRX Series; 15.1X53 versions prior to 15.1X53-D593 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S5. **CVE ID : CVE-2020-1661**		
N/A	16-Oct-20	4.3	On Juniper Networks Junos OS and Junos OS Evolved devices, BGP session flapping can lead to a routing process daemon (RPD) crash and restart, limiting the attack surface to configured BGP peers. This issue only affects devices with BGP damping in combination with accepted-prefix-limit configuration. When the issue occurs the following messages will appear in the /var/log/messages: rpd[6046]: %DAEMON-4-BGP_PREFIX_THRESH_EXCEEDED: XXXX (External AS x): Configured maximum accepted prefix-limit threshold(1800) exceeded for inet6-unicast nlri: 1984 (instance master) rpd[6046]: %DAEMON-3-BGP_CEASE_PREFIX_LIMIT_EXCEEDED: 2001:x:x:x::2	https://kb.juniper.net/JSA11059	O-JUN-JUNO-031120/1120

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(External AS x): Shutting down peer due to exceeding configured maximum accepted prefix-limit(2000) for inet6-unicast nlri: 2001 (instance master) rpd[6046]: %DAEMON-4: bgp_rt_maxprefixes_check_common:9284: NOTIFICATION sent to 2001:x:x:x::2 (External AS x): code 6 (Cease) subcode 1 (Maximum Number of Prefixes Reached) AFI: 2 SAFI: 1 prefix limit 2000 kernel: %KERN-5: mastership_relinquish_on_process_exit: RPD crashed on master RE. Sending SIGUSR2 to chassisd (5612:chassisd) to trigger RE switchover This issue affects: Juniper Networks Junos OS: 17.2R3-S3; 17.3 version 17.3R3-S3 and later versions, prior to 17.3R3-S8; 17.4 version 17.4R2-S4, 17.4R3 and later versions, prior to 17.4R2-S10, 17.4R3-S2; 18.1 version 18.1R3-S6 and later versions, prior to 18.1R3-S10; 18.2 version 18.2R3 and later versions, prior to 18.2R3-S4; 18.2X75 version 18.2X75-D50, 18.2X75-D60 and later versions, prior to 18.2X75-D53, 18.2X75-D65; 18.3 version 18.3R2 and later versions, prior to 18.3R2-S4, 18.3R3-S2; 18.4 version 18.4R2 and later versions, prior to 18.4R2-S5, 18.4R3-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S2; 19.1 version 19.1R1 and later versions, prior to 19.1R2-S2, 19.1R3-S1; 19.2 version 19.2R1 and later versions, prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2; 20.1 versions prior to 20.1R1-S2, 20.1R2. Juniper Networks Junos OS Evolved prior to 20.1R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 17.2R3-S3. **CVE ID : CVE-2020-1662**		
Out-of-bounds Write	16-Oct-20	7.2	A stack buffer overflow vulnerability in the device control daemon (DCD) on Juniper Networks Junos OS allows a low privilege local user to create a Denial of Service (DoS) against the daemon or execute arbitrary code in the system with root privilege. This issue affects Juniper Networks Junos OS: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.2X75 versions prior to 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3-S4; 18.4 versions prior to 18.4R2-S5, 18.4R3-S5; 19.1 versions prior to 19.1R3-S3; 19.2 versions prior to 19.2R1-S5, 19.2R3;	https://kb.juniper.net/JSA11061	O-JUN-JUNO-031120/1121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2-S2, 19.4R3; 20.1 versions prior to 20.1R1-S4, 20.1R2; 20.2 versions prior to 20.2R1-S1, 20.2R2. Versions of Junos OS prior to 17.3 are unaffected by this vulnerability. **CVE ID : CVE-2020-1664**		
N/A	16-Oct-20	5	On Juniper Networks MX Series and EX9200 Series, in a certain condition the IPv6 Distributed Denial of Service (DDoS) protection might not take affect when it reaches the threshold condition. The DDoS protection allows the device to continue to function while it is under DDoS attack, protecting both the Routing Engine (RE) and the Flexible PIC Concentrator (FPC) during the DDoS attack. When this issue occurs, the RE and/or the FPC can become overwhelmed, which could disrupt network protocol operations and/or interrupt traffic. This issue does not affect IPv4 DDoS protection. This issue affects MX Series and EX9200 Series with Trio-based PFEs (Packet Forwarding Engines). Please refer to https://kb.juniper.net/KB25385 for the list of Trio-based PFEs. This issue affects Juniper Networks Junos OS	https://kb.juniper.net/JSA11062	O-JUN-JUNO-031120/1122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on MX series and EX9200 Series: 17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R2-S7, 18.2R3, 18.2R3-S3; 18.2X75 versions prior to 18.2X75-D30; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2. **CVE ID : CVE-2020-1665**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	16-Oct-20	4	When DNS filtering is enabled on Juniper Networks Junos MX Series with one of the following cards MS-PIC, MS-MIC or MS-MPC, an incoming stream of packets processed by the Multiservices PIC Management Daemon (mspmand) process might be bypassed due to a race condition. Due to this vulnerability, mspmand process, responsible for managing "URL Filtering service", can crash, causing the Services PIC to restart. While the Services PIC is restarting, all PIC services including DNS filtering service (DNS sink holing) will be bypassed until the Services PIC completes its boot process. This issue affects Juniper Networks Junos OS: 17.3 versions prior to 17.3R3-S8; 18.3 versions prior to 18.3R3-S1; 18.4	N/A	O-JUN-JUNO-031120/1123

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 18.4R3; 19.1 versions prior to 19.1R3; 19.2 versions prior to 19.2R2; 19.3 versions prior to 19.3R3. This issue does not affect Juniper Networks Junos OS 17.4, 18.1, and 18.2. **CVE ID : CVE-2020-1667**		
Uncontrolled Resource Consumption	16-Oct-20	3.3	On Juniper Networks EX2300 Series, receipt of a stream of specific multicast packets by the layer2 interface can cause high CPU load, which could lead to traffic interruption. This issue occurs when multicast packets are received by the layer 2 interface. To check if the device has high CPU load due to this issue, the administrator can issue the following command: user@host> show chassis routing-engine Routing Engine status: ... Idle 2 percent the "Idle" value shows as low (2 % in the example above), and also the following command: user@host> show system processes summary ... PID USERNAME PRI NICE SIZE RES STATE TIME WCPU COMMAND 11639 root 52 0 283M 11296K select 12:15 44.97% eventd 11803 root 81 0 719M 239M RUN 251:12 31.98% fxpc{fxpc} the eventd and the fxpc processes might use higher WCPU percentage (respectively 44.97% and	https://kb.juniper.net/JSA11065	O-JUN-JUNO-031120/1124

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			31.98% in the above example). This issue affects Juniper Networks Junos OS on EX2300 Series: 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2. **CVE ID : CVE-2020-1668**		
Insufficiently Protected Credentials	16-Oct-20	2.1	The Juniper Device Manager (JDM) container, used by the disaggregated Junos OS architecture on Juniper Networks NFX350 Series devices, stores password hashes in the world-readable file /etc/passwd. This is not a security best current practice as it can allow an attacker with access to the local filesystem the ability to brute-force decrypt password hashes stored on the system. This issue affects Juniper Networks Junos OS on NFX350: 19.4 versions prior to 19.4R3; 20.1 versions prior to 20.1R1-S4, 20.1R2. **CVE ID : CVE-2020-1669**	https://kb.juniper.net/JSA11066	O-JUN-JUNO-031120/1125
Uncontrolled	16-Oct-20	3.3	On Juniper Networks EX4300	N/A	O-JUN-JUNO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource Consumption			Series, receipt of a stream of specific IPv4 packets can cause Routing Engine (RE) high CPU load, which could lead to network protocol operation issue and traffic interruption. This specific packets can originate only from within the broadcast domain where the device is connected. This issue occurs when the packets enter to the IRB interface. Only IPv4 packets can trigger this issue. IPv6 packets cannot trigger this issue. This issue affects Juniper Networks Junos OS on EX4300 series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.1 versions prior to 18.1R3-S10; 18.2 versions prior to 18.2R3-S4; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2; 18.4 versions prior to 18.4R2-S4, 18.4R3-S2; 19.1 versions prior to 19.1R2-S2, 19.1R3-S1; 19.2 versions prior to 19.2R1-S5, 19.2R2-S1, 19.2R3; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2; 20.1 versions prior to 20.1R1-S3, 20.1R2. **CVE ID : CVE-2020-1670**		031120/1126
N/A	16-Oct-20	5	On Juniper Networks Junos OS platforms configured as DHCPv6 local server or DHCPv6 Relay Agent, Juniper	https://kb.juniper.net/JSA11068	O-JUN-JUNO-031120/1127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networks Dynamic Host Configuration Protocol Daemon (JDHCPD) process might crash with a core dump if a malformed DHCPv6 packet is received, resulting with the restart of the daemon. This issue only affects DHCPv6, it does not affect DHCPv4. This issue affects: Juniper Networks Junos OS 17.4 versions prior to 17.4R2-S12, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.2X75 versions prior to 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.2 version 19.2R2 and later versions; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2-S2, 19.4R3; 20.1 versions prior to 20.1R1-S3, 20.1R2; This issue does not affect Juniper Networks Junos OS prior to 17.4R1. **CVE ID : CVE-2020-1671**		
Improper Input Validation	16-Oct-20	5	On Juniper Networks Junos OS devices configured with DHCPv6 relay enabled, receipt of a specific DHCPv6 packet might crash the jdhcpd daemon. The jdhcpd daemon automatically	https://kb.juniper.net/JSA11069	O-JUN-JUNO-031120/1128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			restarts without intervention, but continuous receipt of specific crafted DHCP messages will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. Only DHCPv6 packet can trigger this issue. DHCPv4 packet cannot trigger this issue. This issue affects Juniper Networks Junos OS: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R2-S2, 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R2-S1, 19.2R3; 19.3 versions prior to 19.3R2-S4, 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S3, 20.1R2. **CVE ID : CVE-2020-1672**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Oct-20	7.6	Insufficient Cross-Site Scripting (XSS) protection in Juniper Networks J-Web and web based (HTTP/HTTPS) services allows an unauthenticated attacker to hijack the target user's HTTP/HTTPS session and perform administrative	https://kb.juniper.net/JSA11070	O-JUN-JUNO-031120/1129

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			actions on the Junos device as the targeted user. This issue only affects Juniper Networks Junos OS devices with HTTP/HTTPS services enabled such as J-Web, Web Authentication, Dynamic-VPN (DVPN), Firewall Authentication Pass-Through with Web-Redirect, and Zero Touch Provisioning (ZTP). Junos OS devices with HTTP/HTTPS services disabled are not affected. If HTTP/HTTPS services are enabled, the following command will show the httpd processes: user@device> show system processes | match http 5260 - S 0:00.13 /usr/sbin/httpd-gk -N 5797 - I 0:00.10 /usr/sbin/httpd --config /jail/var/etc/httpd.conf In order to successfully exploit this vulnerability, the attacker needs to convince the device administrator to take action such as clicking the crafted URL sent via phishing email or convince the administrator to input data in the browser console. This issue affects Juniper Networks Junos OS: 18.1 versions prior to 18.1R3-S1; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2; 18.4 versions prior to 18.4R2-S5, 18.4R3-S2; 19.1		

CVSS Scoring Scale	0-1	1-2	2-3	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 prior to 19.1R2-S2, 19.1R3-S1; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2; 20.1 versions prior to 20.1R1-S2, 20.1R2. This issue does not affect Juniper Networks Junos OS prior to 18.1R1. **CVE ID : CVE-2020-1673**		
N/A	16-Oct-20	4.8	Juniper Networks Junos OS and Junos OS Evolved fail to drop/discard delayed MACsec packets (e.g. delayed by more than 2 seconds). Per the specification, called the "bounded receive delay", there should be no replies to delayed MACsec packets. Any MACsec traffic delayed more than 2 seconds should be dropped and late drop counters should increment. Without MACsec delay protection, an attacker could exploit the delay to spoof or decrypt packets. This issue affects: Juniper Networks Junos OS: 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8, 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions	https://kb.juniper.net/JSA11071	O-JUN-JUNO-031120/1130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 18.4R1-S7, 18.4R2-S5, 18.4R3-S3; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2. Juniper Networks Junos OS Evolved: all versions prior to 19.4R3-EVO; 20.1 versions prior to 20.1R2-EVO. This issue does not affect Junos OS versions prior to 16.1R1. **CVE ID : CVE-2020-1674**		
Missing Release of Resource after Effective Lifetime	16-Oct-20	2.9	On Juniper Networks Junos OS and Junos OS Evolved platforms with EVPN configured, receipt of specific BGP packets causes a slow memory leak. If the memory is exhausted the rpd process might crash. If the issue occurs, the memory leak could be seen by executing the "show task memory detail | match policy | match evpn" command multiple times to check if memory (Alloc Blocks value) is increasing. root@device> show task memory detail | match policy | match evpn ---------- Allocator Memory Report ---------- Name | Size | Alloc DTXP Size | Alloc Blocks | Alloc Bytes | MaxAlloc Blocks | MaxAlloc Bytes Policy EVPN Params 20	https://kb.juniper.net/JSA11075	O-JUN-JUNO-031120/1131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			24 3330678 79936272 3330678 79936272 root@device> show task memory detail | match policy | match evpn ---------- Allocator Memory Report ---------- Name | Size | Alloc DTXP Size | Alloc Blocks | Alloc Bytes | MaxAlloc Blocks | MaxAlloc Bytes Policy EVPN Params 20 24 36620255 878886120 36620255 878886120 This issue affects: Juniper Networks Junos OS 19.4 versions prior to 19.4R2; 20.1 versions prior to 20.1R1-S4, 20.1R2; Juniper Networks Junos OS Evolved: 19.4 versions; 20.1 versions prior to 20.1R1-S4-EVO, 20.1R2-EVO; 20.2 versions prior to 20.2R1-EVO; This issue does not affect: Juniper Networks Junos OS releases prior to 19.4R1. Juniper Networks Junos OS Evolved releases prior to 19.4R1-EVO. **CVE ID : CVE-2020-1678**		
N/A	16-Oct-20	4.3	On Juniper Networks PTX and QFX Series devices with packet sampling configured using tunnel-observation mpls-over-udp, sampling of a malformed packet can cause the Kernel Routing Table (KRT) queue to become stuck. KRT is the module within the Routing Process Daemon (RPD) that synchronized the routing	https://kb.juniper.net/JSA11076	O-JUN-JUNO-031120/1132

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			tables with the forwarding tables in the kernel. This table is then synchronized to the Packet Forwarding Engine (PFE) via the KRT queue. Thus, when KRT queue become stuck, it can lead to unexpected packet forwarding issues. An administrator can monitor the following command to check if there is the KRT queue is stuck: user@device > show krt state ... Number of async queue entries: 65007 <--- this value keep on increasing. When this issue occurs, the following message might appear in the /var/log/messages: DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Too many delayed route/nexthop unrefs. Op 2 err 55, rtsm_id 5:-1, msg type 2 DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Memory usage of M_RTNEXTHOP type = (0) Max size possible for M_RTNEXTHOP type = (7297134592) Current delayed unref = (60000), Current unique delayed unref = (18420), Max delayed unref on this platform = (40000) Current delayed weight unref = (60000) Max delayed weight unref on this platform= (400000) curproc = rpd This issue affects Juniper Networks Junos OS		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on PTX/QFX Series: 17.2X75 versions prior to 17.2X75-D105; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.2X75 versions prior to 18.2X75-D420, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R1-S7, 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R2-S2, 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2. This issue does not affect Juniper Networks Junos OS prior to 18.1R1. **CVE ID : CVE-2020-1679**		
Incorrect Calculation of Buffer Size	16-Oct-20	5	On Juniper Networks MX Series with MS-MIC or MS-MPC card configured with NAT64 configuration, receipt of a malformed IPv6 packet may crash the MS-PIC component on MS-MIC or MS-MPC. This issue occurs when a multiservice card is translating the malformed IPv6 packet to IPv4 packet. An unauthenticated attacker can continuously send crafted IPv6 packets through the device causing repetitive MS-PIC process crashes, resulting in an extended Denial of Service condition. This issue	https://kb.juniper.net/JSA11077	O-JUN-JUNO-031120/1133

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
			affects Juniper Networks Junos OS on MX Series: 15.1 versions prior to 15.1R7-S7; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S6; 17.4 versions prior to 17.4R2-S11, 17.4R3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D430, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2. **CVE ID : CVE-2020-1680**		
Improper Input Validation	16-Oct-20	2.1	An input validation vulnerability exists in Juniper Networks Junos OS, allowing an attacker to crash the srxpfe process, causing a Denial of Service (DoS) through the use of specific maintenance commands. The srxpfe process restarts automatically, but continuous execution of the commands could lead to an extended Denial of Service condition. This issue only affects the SRX1500, SRX4100, SRX4200, NFX150, NFX250, and vSRX-based platforms. No other	https://kb.juniper.net/JSA11079	O-JUN-JUNO-031120/1134

CVSS Scoring Scale	0-1	1-2	2-3	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 platforms are affected by this vulnerability. This issue affects Juniper Networks Junos OS: 15.1X49 versions prior to 15.1X49-D220 on SRX1500, SRX4100, SRX4200, vSRX; 17.4 versions prior to 17.4R3-S3 on SRX1500, SRX4100, SRX4200, vSRX; 18.1 versions prior to 18.1R3-S11 on SRX1500, SRX4100, SRX4200, vSRX, NFX150; 18.2 versions prior to 18.2R3-S5 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 19.1 versions prior to 19.1R3-S2 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 19.2 versions prior to 19.2R1-S5, 19.2R3 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250. This issue does not affect Junos OS 19.3 or any subsequent version. **CVE ID : CVE-2020-1682**		
Improper Release of Memory Before Removing Last	16-Oct-20	7.8	On Juniper Networks Junos OS devices, a specific SNMP OID poll causes a memory leak which over time leads to a kernel crash (vmcore). Prior to the kernel crash	https://kb.juniper.net/JSA11080	O-JUN-JUNO-031120/1135

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reference			other processes might be impacted, such as failure to establish SSH connection to the device. The administrator can monitor the output of the following command to check if there is memory leak caused by this issue: user@device> show system virtual-memory | match "pfe_ipc|kmem" pfe_ipc 147 5K - 164352 16,32,64,8192 <-- increasing vm.kmem_map_free: 127246336 <-- decreasing pfe_ipc 0 0K - 18598 32,8192 vm.kmem_map_free: 134582272 This issue affects Juniper Networks Junos OS: 17.4R3; 18.1 version 18.1R3-S5 and later versions prior to 18.1R3-S10; 18.2 version 18.2R3 and later versions prior to 18.2R3-S3; 18.2X75 version 18.2X75-D420, 18.2X75-D50 and later versions prior to 18.2X75-D430, 18.2X75-D53, 18.2X75-D60; 18.3 version 18.3R3 and later versions prior to 18.3R3-S2; 18.4 version 18.4R1-S4, 18.4R2 and later versions prior to 18.4R2-S5, 18.4R3-S1; 19.1 version 19.1R2 and later versions prior to 19.1R2-S2, 19.1R3; 19.2 version 19.2R1 and later versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S5, 19.3R3; 19.4 versions prior to 19.4R1-S3,		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.4R2. This issue does not affect Juniper Networks Junos OS prior to 17.4R3. **CVE ID : CVE-2020-1683**		
Uncontrolled Resource Consumption	16-Oct-20	4.3	On Juniper Networks SRX Series configured with application identification inspection enabled, receipt of specific HTTP traffic can cause high CPU load utilization, which could lead to traffic interruption. Application identification is enabled by default and is automatically turned on when Intrusion Detection and Prevention (IDP), AppFW, AppQoS, or AppTrack is configured. Thus, this issue might occur when IDP, AppFW, AppQoS, or AppTrack is configured. This issue affects Juniper Networks Junos OS on SRX Series: 12.3X48 versions prior to 12.3X48-D105; 15.1X49 versions prior to 15.1X49-D221, 15.1X49-D230; 17.4 versions prior to 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S3; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2; 18.4 versions prior to 18.4R2-S5, 18.4R3-S1; 19.1 versions prior to 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R3; 19.4	https://kb.juniper.net/JSA11081	O-JUN-JUNO-031120/1136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 19.4R2. **CVE ID : CVE-2020-1684**		
Information Exposure Through Discrepancy	16-Oct-20	5	When configuring stateless firewall filters in Juniper Networks EX4600 and QFX 5000 Series devices using Virtual Extensible LAN protocol (VXLAN), the discard action will fail to discard traffic under certain conditions. Given a firewall filter configuration similar to: family ethernet-switching { filter L2-VLAN { term ALLOW { from { user-vlan-id 100; } then { accept; } } term NON-MATCH { then { discard; } } when there is only one term containing a 'user-vlan-id' match condition, and no other terms in the firewall filter except discard, the discard action for non-matching traffic will only discard traffic with the same VLAN ID specified under 'user-vlan-id'. Other traffic (e.g. VLAN ID 200) will not be discarded. This unexpected behavior can lead to unintended traffic passing through the interface where the firewall filter is applied. This issue only affects systems using VXLANs. This issue affects Juniper Networks Junos OS on QFX5K Series: 18.1 versions prior to 18.1R3-S7, except 18.1R3; 18.2 versions prior to 18.2R2-S7, 18.2R3-S1; 18.3	https://kb.juniper.net/JSA11082	O-JUN-JUNO-031120/1137

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 18.3R1-S5, 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R1-S7, 18.4R2-S1, 18.4R3; 19.1 versions prior to 19.1R1-S5, 19.1R2; 19.2 versions prior to 19.2R1-S5, 19.2R2. **CVE ID : CVE-2020-1685**		
N/A	16-Oct-20	7.8	On Juniper Networks Junos OS devices, receipt of a malformed IPv6 packet may cause the system to crash and restart (vmcore). This issue can be trigged by a malformed IPv6 packet destined to the Routing Engine or a transit packet that is sampled using sFlow/jFlow or processed by firewall filter with the syslog and/or log action. An attacker can repeatedly send the offending packet resulting in an extended Denial of Service condition. Only IPv6 packets can trigger this issue. IPv4 packets cannot trigger this issue. This issue affects Juniper Networks Junos OS 18.4 versions prior to 18.4R2-S4, 18.4R3-S1; 19.1 versions prior to 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2. This issue does not affect Juniper Networks Junos OS prior to 18.4R1.	https://kb.juniper.net/JSA11083	O-JUN-JUNO-031120/1138

CVSS Scoring Scale	0-1	1-2	2-3	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-2020-1686		
Uncontrolled Resource Consumption	16-Oct-20	2.9	On Juniper Networks EX4300-MP Series, EX4600 Series and QFX5K Series deployed in (Ethernet VPN) EVPN-(Virtual Extensible LAN) VXLAN configuration, receipt of a stream of specific VXLAN encapsulated layer 2 frames can cause high CPU load, which could lead to network protocol operation issue and traffic interruption. This issue affects devices that are configured as a Layer 2 or Layer 3 gateway of an EVPN-VXLAN deployment. The offending layer 2 frames that cause the issue originate from a different access switch that get encapsulated within the same EVPN-VXLAN domain. This issue affects Juniper Networks Junos OS on EX4300-MP Series, EX4600 Series and QFX5K Series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R2-S2, 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R2-S1, 19.2R3; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4	https://kb.juniper.net/JSA11084	O-JUN-JUNO-031120/1139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 19.4R1-S3, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S3, 20.1R2. **CVE ID : CVE-2020-1687**		
Missing Encryption of Sensitive Data	16-Oct-20	2.1	On Juniper Networks SRX Series and NFX Series, a local authenticated user with access to the shell may obtain the Web API service private key that is used to provide encrypted communication between the Juniper device and the authenticator services. Exploitation of this vulnerability may allow an attacker to decrypt the communications between the Juniper device and the authenticator service. This Web API service is used for authentication services such as the Juniper Identity Management Service, used to obtain user identity for Integrated User Firewall feature, or the integrated ClearPass authentication and enforcement feature. This issue affects Juniper Networks Junos OS on Networks SRX Series and NFX Series: 12.3X48 versions prior to 12.3X48-D105; 15.1X49 versions prior to 15.1X49-D190; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3;	https://kb.juniper.net/JSA11085	O-JUN-JUNO-031120/1140

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.1 versions prior to 18.1R3-S7; 18.2 versions prior to 18.2R3; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R1-S7, 18.4R2; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S4, 19.2R2. **CVE ID : CVE-2020-1688**		
Uncontrolled Resource Consumption	16-Oct-20	3.3	On Juniper Networks EX4300-MP Series, EX4600 Series and QFX5K Series deployed in a Virtual Chassis configuration, receipt of a stream of specific layer 2 frames can cause high CPU load, which could lead to traffic interruption. This issue does not occur when the device is deployed in Stand Alone configuration. The offending layer 2 frame packets can originate only from within the broadcast domain where the device is connected. This issue affects Juniper Networks Junos OS on EX4300-MP Series, EX4600 Series and QFX5K Series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2	https://kb.juniper.net/JSA11086	O-JUN-JUNO-031120/1141

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S3, 20.1R2. **CVE ID : CVE-2020-1689**		
junos_evolved					
Insufficient Session Expiration	16-Oct-20	7.2	The system console configuration option 'log-out-on-disconnect' In Juniper Networks Junos OS Evolved fails to log out an active CLI session when the console cable is disconnected. This could allow a malicious attacker with physical access to the console the ability to resume a previous interactive session and possibly gain administrative privileges. This issue affects all Juniper Networks Junos OS Evolved versions after 18.4R1-EVO, prior to 20.2R1-EVO. **CVE ID : CVE-2020-1666**	https://kb.juniper.net/JSA11063	O-JUN-JUNO-031120/1142
N/A	16-Oct-20	4.8	Juniper Networks Junos OS and Junos OS Evolved fail to drop/discard delayed MACsec packets (e.g. delayed by more than 2 seconds). Per the specification, called the "bounded receive delay", there should be no replies to delayed MACsec packets. Any MACsec traffic delayed more than 2 seconds should be dropped and late drop counters should increment.	https://kb.juniper.net/JSA11071	O-JUN-JUNO-031120/1143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Without MACsec delay protection, an attacker could exploit the delay to spoof or decrypt packets. This issue affects: Juniper Networks Junos OS: 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8, 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R1-S7, 18.4R2-S5, 18.4R3-S3; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2. Juniper Networks Junos OS Evolved: all versions prior to 19.4R3-EVO; 20.1 versions prior to 20.1R2-EVO. This issue does not affect Junos OS versions prior to 16.1R1. **CVE ID : CVE-2020-1674**		
Missing Release of Resource after Effective Lifetime	16-Oct-20	2.9	On Juniper Networks Junos OS and Junos OS Evolved platforms with EVPN configured, receipt of specific BGP packets causes a slow memory leak. If the memory is exhausted the rpd process might crash. If the issue	https://kb.juniper.net/JSA11075	O-JUN-JUNO-031120/1144

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			occurs, the memory leak could be seen by executing the "show task memory detail | match policy | match evpn" command multiple times to check if memory (Alloc Blocks value) is increasing. root@device> show task memory detail | match policy | match evpn ---------- Allocator Memory Report ---------- Name | Size | Alloc DTXP Size | Alloc Blocks | Alloc Bytes | MaxAlloc Blocks | MaxAlloc Bytes Policy EVPN Params 20 24 3330678 79936272 3330678 79936272 root@device> show task memory detail | match policy | match evpn ---------- Allocator Memory Report ---------- Name | Size | Alloc DTXP Size | Alloc Blocks | Alloc Bytes | MaxAlloc Blocks | MaxAlloc Bytes Policy EVPN Params 20 24 36620255 878886120 36620255 878886120 This issue affects: Juniper Networks Junos OS 19.4 versions prior to 19.4R2; 20.1 versions prior to 20.1R1-S4, 20.1R2; Juniper Networks Junos OS Evolved: 19.4 versions; 20.1 versions prior to 20.1R1-S4-EVO, 20.1R2-EVO; 20.2 versions prior to 20.2R1-EVO; This issue does not affect: Juniper Networks Junos OS releases prior to		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.4R1. Juniper Networks Junos OS Evolved releases prior to 19.4R1-EVO. **CVE ID : CVE-2020-1678**		
Improper Handling of Exceptional Conditions	16-Oct-20	3.3	Receipt of a specifically malformed NDP packet sent from the local area network (LAN) to a device running Juniper Networks Junos OS Evolved can cause the ndp process to crash, resulting in a Denial of Service (DoS). The process automatically restarts without intervention, but a continuous receipt of the malformed NDP packets could leaded to an extended Denial of Service condition. During this time, IPv6 neighbor learning will be affected. The issue occurs when parsing the incoming malformed NDP packet. Rather than simply discarding the packet, the process asserts, performing a controlled exit and restart, thereby avoiding any chance of an unhandled exception. Exploitation of this vulnerability is limited to a temporary denial of service, and cannot be leveraged to cause additional impact on the system. This issue is limited to the processing of IPv6 NDP packets. IPv4 packet processing cannot trigger, and is unaffected by this vulnerability. This issue affects all Juniper Networks	https://kb.juniper.net/JSA11078	O-JUN-JUNO-031120/1145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Junos OS Evolved versions prior to 20.1R2-EVO. Junos OS is unaffected by this vulnerability. **CVE ID : CVE-2020-1681**		
Linux					
linux_kernel					
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Oct-20	2.1	An issue was discovered in the Linux kernel before 5.8.15. scalar32_min_max_or in kernel/bpf/verifier.c mishandles bounds tracking during use of 64-bit values, aka CID-5b9fbeb75b6a. **CVE ID : CVE-2020-27194**	N/A	O-LIN-LINU-031120/1146
Uncontrolled Resource Consumption	22-Oct-20	4.9	An issue was discovered in the Linux kernel through 5.9.1, as used with Xen through 4.14.x. Guest OS users can cause a denial of service (host OS hang) via a high rate of events to dom0, aka CID-e99502f76271. **CVE ID : CVE-2020-27673**	N/A	O-LIN-LINU-031120/1147
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Oct-20	6.5	IBM Resilient OnPrem 38.2 could allow a privileged user to inject malicious commands through Python3 scripting. IBM X-Force ID: 185503. **CVE ID : CVE-2020-4636**	https://www.ibm.com/support/pages/node/6348694	O-LIN-LINU-031120/1148
Microsoft					
windows					
N/A	16-Oct-20	3.6	VMware Horizon Client for Windows (5.x before 5.5.0) contains a denial-of-service vulnerability due to a file	N/A	O-MIC-WIND-031120/1149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system access control issue during install time. Successful exploitation of this issue may allow an attacker to overwrite certain admin privileged files through a symbolic link attack at install time. This will result into a denial-of-service condition on the machine where Horizon Client for Windows is installed. **CVE ID : CVE-2020-3991**		
Unquoted Search Path or Element	19-Oct-20	4.6	On Windows the Veyon Service before version 4.4.2 contains an unquoted service path vulnerability, allowing locally authenticated users with administrative privileges to run malicious executables with LocalSystem privileges. Since Veyon users (both students and teachers) usually don't have administrative privileges, this vulnerability is only dangerous in anyway unsafe setups. The problem has been fixed in version 4.4.2. As a workaround, the exploitation of the vulnerability can be prevented by revoking administrative privileges from all potentially untrustworthy users. **CVE ID : CVE-2020-15261**	https://github.com/veyon/veyon/security/advisories/GHSA-c8cc-x786-hqqp	O-MIC-WIND-031120/1150
Out-of-bounds Read	20-Oct-20	6.8	Adobe Illustrator version 24.2 (and earlier) is affected by an out-of-bounds read vulnerability when parsing	N/A	O-MIC-WIND-031120/1151

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted PDF files. This could result in a read past the end of an allocated memory structure, potentially resulting in arbitrary code execution in the context of the current user. This vulnerability requires user interaction to exploit. **CVE ID : CVE-2020-24409**		
Out-of-bounds Read	20-Oct-20	6.8	Adobe Illustrator version 24.2 (and earlier) is affected by an out-of-bounds read vulnerability when parsing crafted PDF files. This could result in a read past the end of an allocated memory structure, potentially resulting in arbitrary code execution in the context of the current user. This vulnerability requires user interaction to exploit. **CVE ID : CVE-2020-24410**	N/A	O-MIC-WIND-031120/1152
Out-of-bounds Write	20-Oct-20	6.8	Adobe Illustrator version 24.2 (and earlier) is affected by an out-of-bounds write vulnerability when handling crafted PDF files. This could result in a write past the end of an allocated memory structure, potentially resulting in arbitrary code execution in the context of the current user. This vulnerability requires user interaction to exploit. **CVE ID : CVE-2020-24411**	N/A	O-MIC-WIND-031120/1153
Improper	20-Oct-20	6.8	Adobe Illustrator version	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			24.1.2 (and earlier) is affected by a memory corruption vulnerability that occurs when parsing a specially crafted .svg file. This could result in arbitrary code execution in the context of the current user. This vulnerability requires user interaction to exploit. **CVE ID : CVE-2020-24412**		031120/1154
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-20	6.8	Adobe Illustrator version 24.1.2 (and earlier) is affected by a memory corruption vulnerability that occurs when parsing a specially crafted .svg file. This could result in arbitrary code execution in the context of the current user. This vulnerability requires user interaction to exploit. **CVE ID : CVE-2020-24413**	N/A	O-MIC-WIND-031120/1155
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Oct-20	6.8	Adobe Illustrator version 24.1.2 (and earlier) is affected by a memory corruption vulnerability that occurs when parsing a specially crafted .svg file. This could result in arbitrary code execution in the context of the current user. This vulnerability requires user interaction to exploit. **CVE ID : CVE-2020-24414**	N/A	O-MIC-WIND-031120/1156
Improper Restriction of Operations	20-Oct-20	6.8	Adobe Illustrator version 24.1.2 (and earlier) is affected by a memory corruption vulnerability that	N/A	O-MIC-WIND-031120/1157

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			occurs when parsing a specially crafted .svg file. This could result in arbitrary code execution in the context of the current user. This vulnerability requires user interaction to exploit. **CVE ID : CVE-2020-24415**		
Out-of-bounds Read	21-Oct-20	9.3	Adobe After Effects version 17.1.1 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted .aepx file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. This vulnerability requires user interaction to exploit. **CVE ID : CVE-2020-24418**	N/A	O-MIC-WIND-031120/1158
Uncontrolled Search Path Element	21-Oct-20	6.9	Adobe After Effects version 17.1.1 (and earlier) for Windows is affected by an uncontrolled search path vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2020-24419**	N/A	O-MIC-WIND-031120/1159
Uncontrolled Search Path Element	21-Oct-20	6.9	Adobe Photoshop for Windows version 21.2.1 (and earlier) is affected by an uncontrolled search path	N/A	O-MIC-WIND-031120/1160

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			element vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2020-24420**		
Uncontrolled Search Path Element	21-Oct-20	6.9	Adobe Media Encoder version 14.4 (and earlier) for Windows is affected by an uncontrolled search path vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2020-24423**	N/A	O-MIC-WIND-031120/1161
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Oct-20	7.5	An issue was discovered in Aptean Product Configurator 4.61.0000 on Windows. A Time based SQL injection affects the nameTxt parameter on the main login page (aka cse?cmd=LOGIN). This can be exploited directly, and remotely. **CVE ID : CVE-2020-26944**	N/A	O-MIC-WIND-031120/1162
Insufficiently Protected Credentials	23-Oct-20	4	VMware Horizon Client for Windows (5.x prior to 5.5.0) contains an information disclosure vulnerability. A malicious attacker with local privileges on the machine where Horizon Client for Windows is installed may be able to retrieve hashed	N/A	O-MIC-WIND-031120/1163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials if the client crashes. **CVE ID : CVE-2020-3998**		
Unrestricted Upload of File with Dangerous Type	30-Oct-20	6.8	IBM i2 iBase 8.9.13 could allow an attacker to upload arbitrary executable files which, when executed by an unsuspecting victim could result in code execution. IBM X-Force ID: 184579. **CVE ID : CVE-2020-4588**	https://www.ibm.com/support/pages/node/6357037	O-MIC-WIND-031120/1164
Weak Password Requirements	27-Oct-20	1.9	Pulse Secure Desktop Client 9.0Rx before 9.0R5 and 9.1Rx before 9.1R4 on Windows reveals users' passwords if Save Settings is enabled. **CVE ID : CVE-2020-8956**	N/A	O-MIC-WIND-031120/1165
Double Free	21-Oct-20	9.3	Adobe Animate version 20.5 (and earlier) is affected by a double free vulnerability when parsing a crafted .fla file, which could result in arbitrary code execution in the context of the current user. This vulnerability requires user interaction to exploit. **CVE ID : CVE-2020-9747**	N/A	O-MIC-WIND-031120/1166
Out-of-bounds Read	21-Oct-20	9.3	Adobe Animate version 20.5 (and earlier) is affected by an out-of-bounds read vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted .fla file in Animate.	N/A	O-MIC-WIND-031120/1167

CVSS Scoring Scale	0-1	1-2	2-3	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-2020-9749		
Out-of-bounds Read	21-Oct-20	9.3	Adobe Animate version 20.5 (and earlier) is affected by an out-of-bounds read vulnerability, which could result in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted .fla file in Animate. **CVE ID : CVE-2020-9750**	N/A	O-MIC-WIND-031120/1168
windows_10					
Improper Privilege Management	16-Oct-20	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-2020-0764**	N/A	O-MIC-WIND-031120/1169
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Oct-20	7.2	An elevation of privilege vulnerability exists when Windows Hyper-V on a host server fails to properly handle objects in memory, aka 'Windows Hyper-V Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1080. **CVE ID : CVE-2020-1047**	N/A	O-MIC-WIND-031120/1170
Improper Restriction of Operations within the Bounds of a Memory	16-Oct-20	7.2	An elevation of privilege vulnerability exists when Windows Hyper-V on a host server fails to properly handle objects in memory, aka 'Windows Hyper-V Elevation of Privilege Vulnerability'. This CVE ID is	N/A	O-MIC-WIND-031120/1171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			unique from CVE-2020-1047. **CVE ID : CVE-2020-1080**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Oct-20	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'. This CVE ID is unique from CVE-2020-16923. **CVE ID : CVE-2020-1167**	N/A	O-MIC-WIND-031120/1172
N/A	16-Oct-20	4.6	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate specific malicious data from a user on a guest operating system.To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application.The security update addresses the vulnerability by resolving the conditions where Hyper-V would fail to handle these requests., aka 'Windows Hyper-V Denial of Service Vulnerability'. **CVE ID : CVE-2020-1243**	N/A	O-MIC-WIND-031120/1173
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Application Compatibility Client Library	N/A	O-MIC-WIND-031120/1174

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improperly handles registry operations, aka 'Windows Application Compatibility Client Library Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16920. **CVE ID : CVE-2020-16876**		
Improper Privilege Management	16-Oct-20	3.6	An elevation of privilege vulnerability exists when Microsoft Windows improperly handles reparse points, aka 'Windows Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16877**	N/A	O-MIC-WIND-031120/1175
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Storage VSP Driver improperly handles file operations, aka 'Windows Storage VSP Driver Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16885**	N/A	O-MIC-WIND-031120/1176
Improper Privilege Management	16-Oct-20	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'. **CVE ID : CVE-2020-16887**	N/A	O-MIC-WIND-031120/1177
Information Exposure	16-Oct-20	2.1	An information disclosure vulnerability exists when the Windows KernelStream improperly handles objects in memory, aka 'Windows	N/A	O-MIC-WIND-031120/1178

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			KernelStream Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16889**		
Improper Privilege Management	16-Oct-20	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16890**	N/A	O-MIC-WIND-031120/1179
Improper Input Validation	16-Oct-20	7.2	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-16891**	N/A	O-MIC-WIND-031120/1180
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists in the way that the Windows kernel image handles objects in memory.An attacker who successfully exploited the vulnerability could execute code with elevated permissions.To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application.The security update addresses the vulnerability by ensuring the Windows kernel image properly handles objects in	N/A	O-MIC-WIND-031120/1181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory., aka 'Windows Image Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16892**		
Improper Input Validation	16-Oct-20	6.8	A remote code execution vulnerability exists when Windows Network Address Translation (NAT) fails to properly handle UDP traffic, aka 'Windows NAT Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-16894**	N/A	O-MIC-WIND-031120/1182
Improper Privilege Management	16-Oct-20	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-2020-16895**	N/A	O-MIC-WIND-031120/1183
Information Exposure	16-Oct-20	5	An information disclosure vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16896**	N/A	O-MIC-WIND-031120/1184
N/A	16-Oct-20	2.1	An information disclosure vulnerability exists when NetBIOS over TCP (NBT) Extensions (NetBT) improperly handle objects in memory, aka 'NetBT	N/A	O-MIC-WIND-031120/1185

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
			Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16897**		
N/A	16-Oct-20	5.8	A remote code execution vulnerability exists when the Windows TCP/IP stack improperly handles ICMPv6 Router Advertisement packets, aka 'Windows TCP/IP Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-16898**	N/A	O-MIC-WIND-031120/1186
N/A	16-Oct-20	7.8	A denial of service vulnerability exists when the Windows TCP/IP stack improperly handles ICMPv6 Router Advertisement packets, aka 'Windows TCP/IP Denial of Service Vulnerability'. **CVE ID : CVE-2020-16899**	N/A	O-MIC-WIND-031120/1187
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Event System improperly handles objects in memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Event System Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16900**	N/A	O-MIC-WIND-031120/1188
Improper Initialization	16-Oct-20	2.1	An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory.To exploit this vulnerability, an	N/A	O-MIC-WIND-031120/1189

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated attacker could run a specially crafted application, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-16938. **CVE ID : CVE-2020-16901**		
Improper Privilege Management	16-Oct-20	7.2	An elevation of privilege vulnerability exists in the Windows Installer when the Windows Installer fails to properly sanitize input leading to an insecure library loading behavior.A locally authenticated attacker could run arbitrary code with elevated system privileges, aka 'Windows Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16902**	N/A	O-MIC-WIND-031120/1190
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16909. **CVE ID : CVE-2020-16905**	N/A	O-MIC-WIND-031120/1191
Improper Privilege Management	16-Oct-20	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k	N/A	O-MIC-WIND-031120/1192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16913. **CVE ID : CVE-2020-16907**		
Improper Privilege Management	16-Oct-20	7.2	An elevation of privilege vulnerability exists in Windows Setup in the way it handles directories.A locally authenticated attacker could run arbitrary code with elevated system privileges, aka 'Windows Setup Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16908**	N/A	O-MIC-WIND-031120/1193
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16905. **CVE ID : CVE-2020-16909**	N/A	O-MIC-WIND-031120/1194
Improper Preservation of Permissions	16-Oct-20	4.3	A security feature bypass vulnerability exists when Microsoft Windows fails to handle file creation permissions, which could allow an attacker to create files in a protected Unified Extensible Firmware Interface (UEFI) location.To exploit this vulnerability, an attacker could run a specially crafted application to bypass	N/A	O-MIC-WIND-031120/1195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Unified Extensible Firmware Interface (UEFI) variable security in Windows.The security update addresses the vulnerability by correcting security feature behavior to enforce permissions., aka 'Windows Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-16910**		
N/A	16-Oct-20	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-2020-16911**	N/A	O-MIC-WIND-031120/1196
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16936, CVE-2020-16972, CVE-2020-16973, CVE-2020-16974, CVE-2020-16975, CVE-2020-16976. **CVE ID : CVE-2020-16912**	N/A	O-MIC-WIND-031120/1197
Improper Privilege Management	16-Oct-20	7.2	An elevation of privilege vulnerability exists in Windows when the Windows	N/A	O-MIC-WIND-031120/1198

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16907. **CVE ID : CVE-2020-16913**		
Information Exposure	16-Oct-20	2.1	An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface Plus (GDI+) handles objects in memory, allowing an attacker to retrieve information from a targeted system, aka 'Windows GDI+ Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16914**	N/A	O-MIC-WIND-031120/1199
Out-of-bounds Write	16-Oct-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. **CVE ID : CVE-2020-16915**	N/A	O-MIC-WIND-031120/1200
Improper Privilege Management	16-Oct-20	7.2	An elevation of privilege vulnerability exists when Windows improperly handles COM object creation, aka 'Windows COM Server Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16935. **CVE ID : CVE-2020-16916**	N/A	O-MIC-WIND-031120/1201

CVSS Scoring Scale	0-1	1-2	2-3	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	16-Oct-20	2.1	An information disclosure vulnerability exists when the Windows Enterprise App Management Service improperly handles certain file operations, aka 'Windows Enterprise App Management Service Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16919**	N/A	O-MIC-WIND-031120/1202
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Application Compatibility Client Library improperly handles registry operations, aka 'Windows Application Compatibility Client Library Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16876. **CVE ID : CVE-2020-16920**	N/A	O-MIC-WIND-031120/1203
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Oct-20	2.1	An information disclosure vulnerability exists in Text Services Framework when it fails to properly handle objects in memory, aka 'Windows Text Services Framework Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16921**	N/A	O-MIC-WIND-031120/1204
Improper Verification of Cryptographic Signature	16-Oct-20	2.1	A spoofing vulnerability exists when Windows incorrectly validates file signatures, aka 'Windows Spoofing Vulnerability'. **CVE ID : CVE-2020-16922**	N/A	O-MIC-WIND-031120/1205
N/A	16-Oct-20	6.8	A remote code execution vulnerability exists in the	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1167. **CVE ID : CVE-2020-16923**		031120/1206
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Oct-20	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-16924**	N/A	O-MIC-WIND-031120/1207
N/A	16-Oct-20	7.8	A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability'. **CVE ID : CVE-2020-16927**	N/A	O-MIC-WIND-031120/1208
Improper Handling of Exceptional Conditions	16-Oct-20	6.8	A security feature bypass vulnerability exists in Microsoft Word software when it fails to properly handle .LNK files, aka 'Microsoft Word Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-16933**	N/A	O-MIC-WIND-031120/1209
Improper Privilege	16-Oct-20	7.2	An elevation of privilege vulnerability exists when Windows improperly handles	N/A	O-MIC-WIND-031120/1210

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			COM object creation, aka 'Windows COM Server Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16916. **CVE ID : CVE-2020-16935**		
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16912, CVE-2020-16972, CVE-2020-16973, CVE-2020-16974, CVE-2020-16975, CVE-2020-16976. **CVE ID : CVE-2020-16936**	N/A	O-MIC-WIND-031120/1211
Information Exposure	16-Oct-20	4.3	An information disclosure vulnerability exists when the .NET Framework improperly handles objects in memory, aka '.NET Framework Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16937**	N/A	O-MIC-WIND-031120/1212
N/A	16-Oct-20	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	N/A	O-MIC-WIND-031120/1213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unique from CVE-2020-16901. **CVE ID : CVE-2020-16938**		
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when Group Policy improperly checks access, aka 'Group Policy Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16939**	N/A	O-MIC-WIND-031120/1214
Improper Privilege Management	16-Oct-20	4.9	An elevation of privilege vulnerability exists when the Windows User Profile Service (ProfSvc) improperly handles junction points, aka 'Windows - User Profile Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16940**	N/A	O-MIC-WIND-031120/1215
Improper Release of Memory Before Removing Last Reference	16-Oct-20	5	A denial of service vulnerability exists in Microsoft Outlook software when the software fails to properly handle objects in memory, aka 'Microsoft Outlook Denial of Service Vulnerability'. **CVE ID : CVE-2020-16949**	N/A	O-MIC-WIND-031120/1216
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Oct-20	9.3	A remote code execution vulnerability exists when the Windows Camera Codec Pack improperly handles objects in memory, aka 'Windows Camera Codec Pack Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-16968.	N/A	O-MIC-WIND-031120/1217

CVSS Scoring Scale	0-1	1-2	2-3	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-2020-16967		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Oct-20	9.3	A remote code execution vulnerability exists when the Windows Camera Codec Pack improperly handles objects in memory, aka 'Windows Camera Codec Pack Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-16967. **CVE ID : CVE-2020-16968**	N/A	O-MIC-WIND-031120/1218
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16912, CVE-2020-16936, CVE-2020-16973, CVE-2020-16974, CVE-2020-16975, CVE-2020-16976. **CVE ID : CVE-2020-16972**	N/A	O-MIC-WIND-031120/1219
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. This	N/A	O-MIC-WIND-031120/1220

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2020-16912, CVE-2020-16936, CVE-2020-16972, CVE-2020-16974, CVE-2020-16975, CVE-2020-16976. **CVE ID : CVE-2020-16973**		
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16912, CVE-2020-16936, CVE-2020-16972, CVE-2020-16973, CVE-2020-16975, CVE-2020-16976. **CVE ID : CVE-2020-16974**	N/A	O-MIC-WIND-031120/1221
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16912, CVE-2020-16936, CVE-2020-16972, CVE-2020-16973, CVE-2020-16974, CVE-2020-16976.	N/A	O-MIC-WIND-031120/1222

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-16975		
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16912, CVE-2020-16936, CVE-2020-16972, CVE-2020-16973, CVE-2020-16974, CVE-2020-16975. **CVE ID : CVE-2020-16976**	N/A	O-MIC-WIND-031120/1223
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Oct-20	6.8	A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka 'Microsoft Windows Codecs Library Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-17022**	N/A	O-MIC-WIND-031120/1224
windows_7					
N/A	16-Oct-20	7.8	A denial of service vulnerability exists in Windows Remote Desktop Service when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Service Denial of Service Vulnerability'. **CVE ID : CVE-2020-16863**	N/A	O-MIC-WIND-031120/1225

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
Improper Privilege Management	16-Oct-20	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'. **CVE ID : CVE-2020-16887**	N/A	O-MIC-WIND-031120/1226
Information Exposure	16-Oct-20	2.1	An information disclosure vulnerability exists when the Windows KernelStream improperly handles objects in memory, aka 'Windows KernelStream Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16889**	N/A	O-MIC-WIND-031120/1227
Improper Input Validation	16-Oct-20	7.2	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-16891**	N/A	O-MIC-WIND-031120/1228
Information Exposure	16-Oct-20	5	An information disclosure vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability'.	N/A	O-MIC-WIND-031120/1229

CVSS Scoring Scale	0-1	1-2	2-3	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-2020-16896		
N/A	16-Oct-20	2.1	An information disclosure vulnerability exists when NetBIOS over TCP (NBT) Extensions (NetBT) improperly handle objects in memory, aka 'NetBT Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16897**	N/A	O-MIC-WIND-031120/1230
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Event System improperly handles objects in memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Event System Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16900**	N/A	O-MIC-WIND-031120/1231
Improper Privilege Management	16-Oct-20	7.2	An elevation of privilege vulnerability exists in the Windows Installer when the Windows Installer fails to properly sanitize input leading to an insecure library loading behavior.A locally authenticated attacker could run arbitrary code with elevated system privileges, aka 'Windows Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16902**	N/A	O-MIC-WIND-031120/1232
N/A	16-Oct-20	9.3	A remote code execution vulnerability exists in the way that the Windows	N/A	O-MIC-WIND-031120/1233

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
			Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-16911**		
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16936, CVE-2020-16972, CVE-2020-16973, CVE-2020-16974, CVE-2020-16975, CVE-2020-16976. **CVE ID : CVE-2020-16912**	N/A	O-MIC-WIND-031120/1234
Information Exposure	16-Oct-20	2.1	An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface Plus (GDI+) handles objects in memory, allowing an attacker to retrieve information from a targeted system, aka 'Windows GDI+ Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16914**	N/A	O-MIC-WIND-031120/1235
Improper Privilege Management	16-Oct-20	7.2	An elevation of privilege vulnerability exists when Windows improperly handles COM object creation, aka	N/A	O-MIC-WIND-031120/1236

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			'Windows COM Server Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16935. **CVE ID : CVE-2020-16916**		
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Application Compatibility Client Library improperly handles registry operations, aka 'Windows Application Compatibility Client Library Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16876. **CVE ID : CVE-2020-16920**	N/A	O-MIC-WIND-031120/1237
Improper Verification of Cryptographic Signature	16-Oct-20	2.1	A spoofing vulnerability exists when Windows incorrectly validates file signatures, aka 'Windows Spoofing Vulnerability'. **CVE ID : CVE-2020-16922**	N/A	O-MIC-WIND-031120/1238
N/A	16-Oct-20	6.8	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'. This CVE ID is unique from CVE-2020-1167. **CVE ID : CVE-2020-16923**	N/A	O-MIC-WIND-031120/1239
Improper Restriction of Operations within the	16-Oct-20	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database	N/A	O-MIC-WIND-031120/1240

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-16924**		
Improper Handling of Exceptional Conditions	16-Oct-20	6.8	A security feature bypass vulnerability exists in Microsoft Word software when it fails to properly handle .LNK files, aka 'Microsoft Word Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-16933**	N/A	O-MIC-WIND-031120/1241
Improper Privilege Management	16-Oct-20	7.2	An elevation of privilege vulnerability exists when Windows improperly handles COM object creation, aka 'Windows COM Server Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16916. **CVE ID : CVE-2020-16935**	N/A	O-MIC-WIND-031120/1242
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16912, CVE-2020-16972, CVE-2020-16973, CVE-2020-16974, CVE-2020-16975, CVE-2020-16976. **CVE ID : CVE-2020-16936**	N/A	O-MIC-WIND-031120/1243

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
Information Exposure	16-Oct-20	4.3	An information disclosure vulnerability exists when the .NET Framework improperly handles objects in memory, aka '.NET Framework Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16937**	N/A	O-MIC-WIND-031120/1244
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when Group Policy improperly checks access, aka 'Group Policy Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16939**	N/A	O-MIC-WIND-031120/1245
Improper Privilege Management	16-Oct-20	4.9	An elevation of privilege vulnerability exists when the Windows User Profile Service (ProfSvc) improperly handles junction points, aka 'Windows - User Profile Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16940**	N/A	O-MIC-WIND-031120/1246
Improper Release of Memory Before Removing Last Reference	16-Oct-20	5	A denial of service vulnerability exists in Microsoft Outlook software when the software fails to properly handle objects in memory, aka 'Microsoft Outlook Denial of Service Vulnerability'. **CVE ID : CVE-2020-16949**	N/A	O-MIC-WIND-031120/1247
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker	N/A	O-MIC-WIND-031120/1248

CVSS Scoring Scale	0-1	1-2	2-3	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 gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16912, CVE-2020-16936, CVE-2020-16973, CVE-2020-16974, CVE-2020-16975, CVE-2020-16976. **CVE ID : CVE-2020-16972**		
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16912, CVE-2020-16936, CVE-2020-16972, CVE-2020-16974, CVE-2020-16975, CVE-2020-16976. **CVE ID : CVE-2020-16973**	N/A	O-MIC-WIND-031120/1249
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-	N/A	O-MIC-WIND-031120/1250

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-16912, CVE-2020-16936, CVE-2020-16972, CVE-2020-16973, CVE-2020-16975, CVE-2020-16976. **CVE ID : CVE-2020-16974**		
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16912, CVE-2020-16936, CVE-2020-16972, CVE-2020-16973, CVE-2020-16974, CVE-2020-16976. **CVE ID : CVE-2020-16975**	N/A	O-MIC-WIND-031120/1251
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16912, CVE-2020-16936, CVE-2020-16972, CVE-2020-16973, CVE-2020-16974, CVE-2020-16975. **CVE ID : CVE-2020-16976**	N/A	O-MIC-WIND-031120/1252

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
windows_8.1					
Improper Privilege Management	16-Oct-20	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'. **CVE ID : CVE-2020-16887**	N/A	O-MIC-WIND-031120/1253
Information Exposure	16-Oct-20	2.1	An information disclosure vulnerability exists when the Windows KernelStream improperly handles objects in memory, aka 'Windows KernelStream Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16889**	N/A	O-MIC-WIND-031120/1254
Improper Input Validation	16-Oct-20	7.2	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-16891**	N/A	O-MIC-WIND-031120/1255
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists in the way that the Windows kernel image handles objects in memory.An attacker who successfully exploited the vulnerability could execute code with elevated permissions.To exploit the	N/A	O-MIC-WIND-031120/1256

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability, a locally authenticated attacker could run a specially crafted application.The security update addresses the vulnerability by ensuring the Windows kernel image properly handles objects in memory., aka 'Windows Image Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16892**		
Information Exposure	16-Oct-20	5	An information disclosure vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16896**	N/A	O-MIC-WIND-031120/1257
N/A	16-Oct-20	2.1	An information disclosure vulnerability exists when NetBIOS over TCP (NBT) Extensions (NetBT) improperly handle objects in memory, aka 'NetBT Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16897**	N/A	O-MIC-WIND-031120/1258
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Event System improperly handles objects in memory.To exploit this vulnerability, an attacker would first have to gain	N/A	O-MIC-WIND-031120/1259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution on the victim system, aka 'Windows Event System Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16900**		
Improper Privilege Management	16-Oct-20	7.2	An elevation of privilege vulnerability exists in the Windows Installer when the Windows Installer fails to properly sanitize input leading to an insecure library loading behavior.A locally authenticated attacker could run arbitrary code with elevated system privileges, aka 'Windows Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16902**	N/A	O-MIC-WIND-031120/1260
N/A	16-Oct-20	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-2020-16911**	N/A	O-MIC-WIND-031120/1261
Information Exposure	16-Oct-20	2.1	An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface Plus (GDI+) handles objects in memory, allowing an attacker to retrieve information from a targeted system, aka 'Windows GDI+ Information Disclosure Vulnerability'.	N/A	O-MIC-WIND-031120/1262

CVSS Scoring Scale	0-1	1-2	2-3	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-2020-16914		
Improper Privilege Management	16-Oct-20	7.2	An elevation of privilege vulnerability exists when Windows improperly handles COM object creation, aka 'Windows COM Server Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16935. **CVE ID : CVE-2020-16916**	N/A	O-MIC-WIND-031120/1263
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Application Compatibility Client Library improperly handles registry operations, aka 'Windows Application Compatibility Client Library Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16876. **CVE ID : CVE-2020-16920**	N/A	O-MIC-WIND-031120/1264
Improper Verification of Cryptographic Signature	16-Oct-20	2.1	A spoofing vulnerability exists when Windows incorrectly validates file signatures, aka 'Windows Spoofing Vulnerability'. **CVE ID : CVE-2020-16922**	N/A	O-MIC-WIND-031120/1265
N/A	16-Oct-20	6.8	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'. This CVE ID is unique from CVE-2020-1167.	N/A	O-MIC-WIND-031120/1266

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
			CVE ID : CVE-2020-16923		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Oct-20	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-16924**	N/A	O-MIC-WIND-031120/1267
N/A	16-Oct-20	7.8	A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability'. **CVE ID : CVE-2020-16927**	N/A	O-MIC-WIND-031120/1268
Improper Handling of Exceptional Conditions	16-Oct-20	6.8	A security feature bypass vulnerability exists in Microsoft Word software when it fails to properly handle .LNK files, aka 'Microsoft Word Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-16933**	N/A	O-MIC-WIND-031120/1269
Improper Privilege Management	16-Oct-20	7.2	An elevation of privilege vulnerability exists when Windows improperly handles COM object creation, aka 'Windows COM Server Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16916.	N/A	O-MIC-WIND-031120/1270

CVSS Scoring Scale	0-1	1-2	2-3	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-2020-16935		
Information Exposure	16-Oct-20	4.3	An information disclosure vulnerability exists when the .NET Framework improperly handles objects in memory, aka '.NET Framework Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16937**	N/A	O-MIC-WIND-031120/1271
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when Group Policy improperly checks access, aka 'Group Policy Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16939**	N/A	O-MIC-WIND-031120/1272
Improper Privilege Management	16-Oct-20	4.9	An elevation of privilege vulnerability exists when the Windows User Profile Service (ProfSvc) improperly handles junction points, aka 'Windows - User Profile Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16940**	N/A	O-MIC-WIND-031120/1273
Improper Release of Memory Before Removing Last Reference	16-Oct-20	5	A denial of service vulnerability exists in Microsoft Outlook software when the software fails to properly handle objects in memory, aka 'Microsoft Outlook Denial of Service Vulnerability'. **CVE ID : CVE-2020-16949**	N/A	O-MIC-WIND-031120/1274
windows_rt_8.1					
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists in the way that the Windows	N/A	O-MIC-WIND-031120/1275

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'. **CVE ID : CVE-2020-16887**		
Information Exposure	16-Oct-20	2.1	An information disclosure vulnerability exists when the Windows KernelStream improperly handles objects in memory, aka 'Windows KernelStream Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16889**	N/A	O-MIC-WIND-031120/1276
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists in the way that the Windows kernel image handles objects in memory.An attacker who successfully exploited the vulnerability could execute code with elevated permissions.To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application.The security update addresses the vulnerability by ensuring the Windows kernel image properly handles objects in memory., aka 'Windows Image Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16892**	N/A	O-MIC-WIND-031120/1277
Information Exposure	16-Oct-20	5	An information disclosure vulnerability exists in Remote Desktop Protocol (RDP)	N/A	O-MIC-WIND-031120/1278

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16896**		
N/A	16-Oct-20	2.1	An information disclosure vulnerability exists when NetBIOS over TCP (NBT) Extensions (NetBT) improperly handle objects in memory, aka 'NetBT Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16897**	N/A	O-MIC-WIND-031120/1279
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Event System improperly handles objects in memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Event System Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16900**	N/A	O-MIC-WIND-031120/1280
Improper Privilege Management	16-Oct-20	7.2	An elevation of privilege vulnerability exists in the Windows Installer when the Windows Installer fails to properly sanitize input leading to an insecure library loading behavior.A locally authenticated attacker could run arbitrary code with elevated system privileges,	N/A	O-MIC-WIND-031120/1281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			aka 'Windows Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16902**		
N/A	16-Oct-20	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-2020-16911**	N/A	O-MIC-WIND-031120/1282
Information Exposure	16-Oct-20	2.1	An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface Plus (GDI+) handles objects in memory, allowing an attacker to retrieve information from a targeted system, aka 'Windows GDI+ Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16914**	N/A	O-MIC-WIND-031120/1283
Improper Privilege Management	16-Oct-20	7.2	An elevation of privilege vulnerability exists when Windows improperly handles COM object creation, aka 'Windows COM Server Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16935. **CVE ID : CVE-2020-16916**	N/A	O-MIC-WIND-031120/1284
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Application Compatibility Client Library	N/A	O-MIC-WIND-031120/1285

CVSS Scoring Scale	0-1	1-2	2-3	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 registry operations, aka 'Windows Application Compatibility Client Library Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16876. **CVE ID : CVE-2020-16920**		
Improper Verification of Cryptographic Signature	16-Oct-20	2.1	A spoofing vulnerability exists when Windows incorrectly validates file signatures, aka 'Windows Spoofing Vulnerability'. **CVE ID : CVE-2020-16922**	N/A	O-MIC-WIND-031120/1286
N/A	16-Oct-20	6.8	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'. This CVE ID is unique from CVE-2020-1167. **CVE ID : CVE-2020-16923**	N/A	O-MIC-WIND-031120/1287
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Oct-20	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-16924**	N/A	O-MIC-WIND-031120/1288
N/A	16-Oct-20	7.8	A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows	N/A	O-MIC-WIND-031120/1289

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
			Remote Desktop Protocol (RDP) Denial of Service Vulnerability'. **CVE ID : CVE-2020-16927**		
Improper Handling of Exceptional Conditions	16-Oct-20	6.8	A security feature bypass vulnerability exists in Microsoft Word software when it fails to properly handle .LNK files, aka 'Microsoft Word Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-16933**	N/A	O-MIC-WIND-031120/1290
Improper Privilege Management	16-Oct-20	7.2	An elevation of privilege vulnerability exists when Windows improperly handles COM object creation, aka 'Windows COM Server Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16916. **CVE ID : CVE-2020-16935**	N/A	O-MIC-WIND-031120/1291
Information Exposure	16-Oct-20	4.3	An information disclosure vulnerability exists when the .NET Framework improperly handles objects in memory, aka '.NET Framework Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16937**	N/A	O-MIC-WIND-031120/1292
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when Group Policy improperly checks access, aka 'Group Policy Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16939**	N/A	O-MIC-WIND-031120/1293

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	16-Oct-20	4.9	An elevation of privilege vulnerability exists when the Windows User Profile Service (ProfSvc) improperly handles junction points, aka 'Windows - User Profile Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16940**	N/A	O-MIC-WIND-031120/1294
Improper Release of Memory Before Removing Last Reference	16-Oct-20	5	A denial of service vulnerability exists in Microsoft Outlook software when the software fails to properly handle objects in memory, aka 'Microsoft Outlook Denial of Service Vulnerability'. **CVE ID : CVE-2020-16949**	N/A	O-MIC-WIND-031120/1295
windows_server_2008					
N/A	16-Oct-20	7.8	A denial of service vulnerability exists in Windows Remote Desktop Service when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Service Denial of Service Vulnerability'. **CVE ID : CVE-2020-16863**	N/A	O-MIC-WIND-031120/1296
Improper Privilege Management	16-Oct-20	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-031120/1297

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
			CVE ID : CVE-2020-16887		
Information Exposure	16-Oct-20	2.1	An information disclosure vulnerability exists when the Windows KernelStream improperly handles objects in memory, aka 'Windows KernelStream Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16889**	N/A	O-MIC-WIND-031120/1298
Improper Input Validation	16-Oct-20	7.2	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-16891**	N/A	O-MIC-WIND-031120/1299
Information Exposure	16-Oct-20	5	An information disclosure vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16896**	N/A	O-MIC-WIND-031120/1300
N/A	16-Oct-20	2.1	An information disclosure vulnerability exists when NetBIOS over TCP (NBT) Extensions (NetBT) improperly handle objects in memory, aka 'NetBT Information Disclosure Vulnerability'.	N/A	O-MIC-WIND-031120/1301

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-16897		
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Event System improperly handles objects in memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Event System Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16900**	N/A	O-MIC-WIND-031120/1302
Improper Privilege Management	16-Oct-20	7.2	An elevation of privilege vulnerability exists in the Windows Installer when the Windows Installer fails to properly sanitize input leading to an insecure library loading behavior.A locally authenticated attacker could run arbitrary code with elevated system privileges, aka 'Windows Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16902**	N/A	O-MIC-WIND-031120/1303
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16936, CVE-2020-	N/A	O-MIC-WIND-031120/1304

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			16972, CVE-2020-16973, CVE-2020-16974, CVE-2020-16975, CVE-2020-16976. **CVE ID : CVE-2020-16912**		
Information Exposure	16-Oct-20	2.1	An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface Plus (GDI+) handles objects in memory, allowing an attacker to retrieve information from a targeted system, aka 'Windows GDI+ Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16914**	N/A	O-MIC-WIND-031120/1305
Improper Privilege Management	16-Oct-20	7.2	An elevation of privilege vulnerability exists when Windows improperly handles COM object creation, aka 'Windows COM Server Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16935. **CVE ID : CVE-2020-16916**	N/A	O-MIC-WIND-031120/1306
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Application Compatibility Client Library improperly handles registry operations, aka 'Windows Application Compatibility Client Library Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16876. **CVE ID : CVE-2020-16920**	N/A	O-MIC-WIND-031120/1307

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
Improper Verification of Cryptographic Signature	16-Oct-20	2.1	A spoofing vulnerability exists when Windows incorrectly validates file signatures, aka 'Windows Spoofing Vulnerability'. **CVE ID : CVE-2020-16922**	N/A	O-MIC-WIND-031120/1308
N/A	16-Oct-20	6.8	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'. This CVE ID is unique from CVE-2020-1167. **CVE ID : CVE-2020-16923**	N/A	O-MIC-WIND-031120/1309
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Oct-20	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-16924**	N/A	O-MIC-WIND-031120/1310
Improper Handling of Exceptional Conditions	16-Oct-20	6.8	A security feature bypass vulnerability exists in Microsoft Word software when it fails to properly handle .LNK files, aka 'Microsoft Word Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-16933**	N/A	O-MIC-WIND-031120/1311
Improper Privilege Management	16-Oct-20	7.2	An elevation of privilege vulnerability exists when Windows improperly handles COM object creation, aka 'Windows COM Server Elevation of Privilege	N/A	O-MIC-WIND-031120/1312

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
			Vulnerability'. This CVE ID is unique from CVE-2020-16916. **CVE ID : CVE-2020-16935**		
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16912, CVE-2020-16972, CVE-2020-16973, CVE-2020-16974, CVE-2020-16975, CVE-2020-16976. **CVE ID : CVE-2020-16936**	N/A	O-MIC-WIND-031120/1313
Information Exposure	16-Oct-20	4.3	An information disclosure vulnerability exists when the .NET Framework improperly handles objects in memory, aka '.NET Framework Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16937**	N/A	O-MIC-WIND-031120/1314
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when Group Policy improperly checks access, aka 'Group Policy Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16939**	N/A	O-MIC-WIND-031120/1315
Improper Privilege	16-Oct-20	4.9	An elevation of privilege vulnerability exists when the Windows User Profile Service	N/A	O-MIC-WIND-031120/1316

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			(ProfSvc) improperly handles junction points, aka 'Windows - User Profile Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16940**		
Improper Release of Memory Before Removing Last Reference	16-Oct-20	5	A denial of service vulnerability exists in Microsoft Outlook software when the software fails to properly handle objects in memory, aka 'Microsoft Outlook Denial of Service Vulnerability'. **CVE ID : CVE-2020-16949**	N/A	O-MIC-WIND-031120/1317
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16912, CVE-2020-16936, CVE-2020-16973, CVE-2020-16974, CVE-2020-16975, CVE-2020-16976. **CVE ID : CVE-2020-16972**	N/A	O-MIC-WIND-031120/1318
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain	N/A	O-MIC-WIND-031120/1319

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16912, CVE-2020-16936, CVE-2020-16972, CVE-2020-16974, CVE-2020-16975, CVE-2020-16976. **CVE ID : CVE-2020-16973**		
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16912, CVE-2020-16936, CVE-2020-16972, CVE-2020-16973, CVE-2020-16975, CVE-2020-16976. **CVE ID : CVE-2020-16974**	N/A	O-MIC-WIND-031120/1320
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16912, CVE-2020-	N/A	O-MIC-WIND-031120/1321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			16936, CVE-2020-16972, CVE-2020-16973, CVE-2020-16974, CVE-2020-16976. **CVE ID : CVE-2020-16975**		
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16912, CVE-2020-16936, CVE-2020-16972, CVE-2020-16973, CVE-2020-16974, CVE-2020-16975. **CVE ID : CVE-2020-16976**	N/A	O-MIC-WIND-031120/1322
windows_server_2012					
Improper Privilege Management	16-Oct-20	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'. **CVE ID : CVE-2020-16887**	N/A	O-MIC-WIND-031120/1323
Information Exposure	16-Oct-20	2.1	An information disclosure vulnerability exists when the Windows KernelStream improperly handles objects in memory, aka 'Windows KernelStream Information Disclosure Vulnerability'.	N/A	O-MIC-WIND-031120/1324

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-16889		
Improper Input Validation	16-Oct-20	7.2	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-16891**	N/A	O-MIC-WIND-031120/1325
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists in the way that the Windows kernel image handles objects in memory.An attacker who successfully exploited the vulnerability could execute code with elevated permissions.To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application.The security update addresses the vulnerability by ensuring the Windows kernel image properly handles objects in memory., aka 'Windows Image Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16892**	N/A	O-MIC-WIND-031120/1326
Information Exposure	16-Oct-20	5	An information disclosure vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows	N/A	O-MIC-WIND-031120/1327

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
			Remote Desktop Protocol (RDP) Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16896**		
N/A	16-Oct-20	2.1	An information disclosure vulnerability exists when NetBIOS over TCP (NBT) Extensions (NetBT) improperly handle objects in memory, aka 'NetBT Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16897**	N/A	O-MIC-WIND-031120/1328
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Event System improperly handles objects in memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Event System Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16900**	N/A	O-MIC-WIND-031120/1329
Improper Privilege Management	16-Oct-20	7.2	An elevation of privilege vulnerability exists in the Windows Installer when the Windows Installer fails to properly sanitize input leading to an insecure library loading behavior.A locally authenticated attacker could run arbitrary code with elevated system privileges, aka 'Windows Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16902**	N/A	O-MIC-WIND-031120/1330

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Oct-20	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-2020-16911**	N/A	O-MIC-WIND-031120/1331
Information Exposure	16-Oct-20	2.1	An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface Plus (GDI+) handles objects in memory, allowing an attacker to retrieve information from a targeted system, aka 'Windows GDI+ Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16914**	N/A	O-MIC-WIND-031120/1332
Improper Privilege Management	16-Oct-20	7.2	An elevation of privilege vulnerability exists when Windows improperly handles COM object creation, aka 'Windows COM Server Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16935. **CVE ID : CVE-2020-16916**	N/A	O-MIC-WIND-031120/1333
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Application Compatibility Client Library improperly handles registry operations, aka 'Windows Application Compatibility Client Library Elevation of	N/A	O-MIC-WIND-031120/1334

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
			Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16876. **CVE ID : CVE-2020-16920**		
Improper Verification of Cryptographic Signature	16-Oct-20	2.1	A spoofing vulnerability exists when Windows incorrectly validates file signatures, aka 'Windows Spoofing Vulnerability'. **CVE ID : CVE-2020-16922**	N/A	O-MIC-WIND-031120/1335
N/A	16-Oct-20	6.8	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'. This CVE ID is unique from CVE-2020-1167. **CVE ID : CVE-2020-16923**	N/A	O-MIC-WIND-031120/1336
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Oct-20	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-16924**	N/A	O-MIC-WIND-031120/1337
N/A	16-Oct-20	7.8	A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability'.	N/A	O-MIC-WIND-031120/1338

CVSS Scoring Scale	0-1	1-2	2-3	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-2020-16927		
Improper Handling of Exceptional Conditions	16-Oct-20	6.8	A security feature bypass vulnerability exists in Microsoft Word software when it fails to properly handle .LNK files, aka 'Microsoft Word Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-16933**	N/A	O-MIC-WIND-031120/1339
Improper Privilege Management	16-Oct-20	7.2	An elevation of privilege vulnerability exists when Windows improperly handles COM object creation, aka 'Windows COM Server Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16916. **CVE ID : CVE-2020-16935**	N/A	O-MIC-WIND-031120/1340
Information Exposure	16-Oct-20	4.3	An information disclosure vulnerability exists when the .NET Framework improperly handles objects in memory, aka '.NET Framework Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16937**	N/A	O-MIC-WIND-031120/1341
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when Group Policy improperly checks access, aka 'Group Policy Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16939**	N/A	O-MIC-WIND-031120/1342
Improper Privilege Management	16-Oct-20	4.9	An elevation of privilege vulnerability exists when the Windows User Profile Service	N/A	O-MIC-WIND-031120/1343

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(ProfSvc) improperly handles junction points, aka 'Windows - User Profile Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16940**		
Improper Release of Memory Before Removing Last Reference	16-Oct-20	5	A denial of service vulnerability exists in Microsoft Outlook software when the software fails to properly handle objects in memory, aka 'Microsoft Outlook Denial of Service Vulnerability'. **CVE ID : CVE-2020-16949**	N/A	O-MIC-WIND-031120/1344
Improper Privilege Management	16-Oct-20	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-2020-16980**	N/A	O-MIC-WIND-031120/1345
windows_server_2016					
Improper Privilege Management	16-Oct-20	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-2020-0764**	N/A	O-MIC-WIND-031120/1346
Improper Restriction of Operations within the Bounds of a	16-Oct-20	7.2	An elevation of privilege vulnerability exists when Windows Hyper-V on a host server fails to properly handle objects in memory, aka 'Windows Hyper-V	N/A	O-MIC-WIND-031120/1347

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1080. **CVE ID : CVE-2020-1047**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Oct-20	7.2	An elevation of privilege vulnerability exists when Windows Hyper-V on a host server fails to properly handle objects in memory, aka 'Windows Hyper-V Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1047. **CVE ID : CVE-2020-1080**	N/A	O-MIC-WIND-031120/1348
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Oct-20	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'. This CVE ID is unique from CVE-2020-16923. **CVE ID : CVE-2020-1167**	N/A	O-MIC-WIND-031120/1349
N/A	16-Oct-20	4.6	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate specific malicious data from a user on a guest operating system.To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application.The security	N/A	O-MIC-WIND-031120/1350

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			update addresses the vulnerability by resolving the conditions where Hyper-V would fail to handle these requests., aka 'Windows Hyper-V Denial of Service Vulnerability'. **CVE ID : CVE-2020-1243**		
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Application Compatibility Client Library improperly handles registry operations, aka 'Windows Application Compatibility Client Library Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16920. **CVE ID : CVE-2020-16876**	N/A	O-MIC-WIND-031120/1351
Improper Privilege Management	16-Oct-20	3.6	An elevation of privilege vulnerability exists when Microsoft Windows improperly handles reparse points, aka 'Windows Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16877**	N/A	O-MIC-WIND-031120/1352
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Storage VSP Driver improperly handles file operations, aka 'Windows Storage VSP Driver Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16885**	N/A	O-MIC-WIND-031120/1353
Improper Privilege	16-Oct-20	4.6	An elevation of privilege vulnerability exists in the way that the Windows	N/A	O-MIC-WIND-031120/1354

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Network Connections Service handles objects in memory, aka 'Windows Network Connections Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16887**		
Information Exposure	16-Oct-20	2.1	An information disclosure vulnerability exists when the Windows KernelStream improperly handles objects in memory, aka 'Windows KernelStream Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16889**	N/A	O-MIC-WIND-031120/1355
Improper Privilege Management	16-Oct-20	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16890**	N/A	O-MIC-WIND-031120/1356
Improper Input Validation	16-Oct-20	7.2	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-16891**	N/A	O-MIC-WIND-031120/1357
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists in the way that the Windows kernel image handles objects in memory.An attacker who	N/A	O-MIC-WIND-031120/1358

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successfully exploited the vulnerability could execute code with elevated permissions.To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application.The security update addresses the vulnerability by ensuring the Windows kernel image properly handles objects in memory., aka 'Windows Image Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16892**		
Improper Input Validation	16-Oct-20	6.8	A remote code execution vulnerability exists when Windows Network Address Translation (NAT) fails to properly handle UDP traffic, aka 'Windows NAT Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-16894**	N/A	O-MIC-WIND-031120/1359
Improper Privilege Management	16-Oct-20	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-2020-16895**	N/A	O-MIC-WIND-031120/1360
Information Exposure	16-Oct-20	5	An information disclosure vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP	N/A	O-MIC-WIND-031120/1361

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16896**		
N/A	16-Oct-20	2.1	An information disclosure vulnerability exists when NetBIOS over TCP (NBT) Extensions (NetBT) improperly handle objects in memory, aka 'NetBT Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16897**	N/A	O-MIC-WIND-031120/1362
N/A	16-Oct-20	5.8	A remote code execution vulnerability exists when the Windows TCP/IP stack improperly handles ICMPv6 Router Advertisement packets, aka 'Windows TCP/IP Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-16898**	N/A	O-MIC-WIND-031120/1363
N/A	16-Oct-20	7.8	A denial of service vulnerability exists when the Windows TCP/IP stack improperly handles ICMPv6 Router Advertisement packets, aka 'Windows TCP/IP Denial of Service Vulnerability'. **CVE ID : CVE-2020-16899**	N/A	O-MIC-WIND-031120/1364
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Event System improperly handles objects in memory.To exploit this vulnerability, an attacker	N/A	O-MIC-WIND-031120/1365

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			would first have to gain execution on the victim system, aka 'Windows Event System Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16900**		
Improper Initialization	16-Oct-20	2.1	An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory.To exploit this vulnerability, an authenticated attacker could run a specially crafted application, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2020-16938. **CVE ID : CVE-2020-16901**	N/A	O-MIC-WIND-031120/1366
Improper Privilege Management	16-Oct-20	7.2	An elevation of privilege vulnerability exists in the Windows Installer when the Windows Installer fails to properly sanitize input leading to an insecure library loading behavior.A locally authenticated attacker could run arbitrary code with elevated system privileges, aka 'Windows Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16902**	N/A	O-MIC-WIND-031120/1367
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka	N/A	O-MIC-WIND-031120/1368

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			'Windows Error Reporting Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16909. **CVE ID : CVE-2020-16905**		
Improper Privilege Management	16-Oct-20	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16913. **CVE ID : CVE-2020-16907**	N/A	O-MIC-WIND-031120/1369
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16905. **CVE ID : CVE-2020-16909**	N/A	O-MIC-WIND-031120/1370
Improper Preservation of Permissions	16-Oct-20	4.3	A security feature bypass vulnerability exists when Microsoft Windows fails to handle file creation permissions, which could allow an attacker to create files in a protected Unified Extensible Firmware Interface (UEFI) location.To exploit this vulnerability, an attacker could run a specially	N/A	O-MIC-WIND-031120/1371

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted application to bypass Unified Extensible Firmware Interface (UEFI) variable security in Windows.The security update addresses the vulnerability by correcting security feature behavior to enforce permissions., aka 'Windows Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-16910**		
N/A	16-Oct-20	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-2020-16911**	N/A	O-MIC-WIND-031120/1372
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16936, CVE-2020-16972, CVE-2020-16973, CVE-2020-16974, CVE-2020-16975, CVE-2020-16976. **CVE ID : CVE-2020-16912**	N/A	O-MIC-WIND-031120/1373
Improper Privilege	16-Oct-20	7.2	An elevation of privilege vulnerability exists in	N/A	O-MIC-WIND-031120/1374

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16907. **CVE ID : CVE-2020-16913**		
Information Exposure	16-Oct-20	2.1	An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface Plus (GDI+) handles objects in memory, allowing an attacker to retrieve information from a targeted system, aka 'Windows GDI+ Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16914**	N/A	O-MIC-WIND-031120/1375
Out-of-bounds Write	16-Oct-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. **CVE ID : CVE-2020-16915**	N/A	O-MIC-WIND-031120/1376
Improper Privilege Management	16-Oct-20	7.2	An elevation of privilege vulnerability exists when Windows improperly handles COM object creation, aka 'Windows COM Server Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16935. **CVE ID : CVE-2020-16916**	N/A	O-MIC-WIND-031120/1377

CVSS Scoring Scale	0-1	1-2	2-3	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	16-Oct-20	2.1	An information disclosure vulnerability exists when the Windows Enterprise App Management Service improperly handles certain file operations, aka 'Windows Enterprise App Management Service Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16919**	N/A	O-MIC-WIND-031120/1378
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Application Compatibility Client Library improperly handles registry operations, aka 'Windows Application Compatibility Client Library Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16876. **CVE ID : CVE-2020-16920**	N/A	O-MIC-WIND-031120/1379
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Oct-20	2.1	An information disclosure vulnerability exists in Text Services Framework when it fails to properly handle objects in memory, aka 'Windows Text Services Framework Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16921**	N/A	O-MIC-WIND-031120/1380
Improper Verification of Cryptographic Signature	16-Oct-20	2.1	A spoofing vulnerability exists when Windows incorrectly validates file signatures, aka 'Windows Spoofing Vulnerability'. **CVE ID : CVE-2020-16922**	N/A	O-MIC-WIND-031120/1381
N/A	16-Oct-20	6.8	A remote code execution vulnerability exists in the	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1167. **CVE ID : CVE-2020-16923**		031120/1382
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Oct-20	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-16924**	N/A	O-MIC-WIND-031120/1383
N/A	16-Oct-20	7.8	A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability'. **CVE ID : CVE-2020-16927**	N/A	O-MIC-WIND-031120/1384
Improper Handling of Exceptional Conditions	16-Oct-20	6.8	A security feature bypass vulnerability exists in Microsoft Word software when it fails to properly handle .LNK files, aka 'Microsoft Word Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-16933**	N/A	O-MIC-WIND-031120/1385
Improper Privilege	16-Oct-20	7.2	An elevation of privilege vulnerability exists when Windows improperly handles	N/A	O-MIC-WIND-031120/1386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			COM object creation, aka 'Windows COM Server Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16916. **CVE ID : CVE-2020-16935**		
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16912, CVE-2020-16972, CVE-2020-16973, CVE-2020-16974, CVE-2020-16975, CVE-2020-16976. **CVE ID : CVE-2020-16936**	N/A	O-MIC-WIND-031120/1387
Information Exposure	16-Oct-20	4.3	An information disclosure vulnerability exists when the .NET Framework improperly handles objects in memory, aka '.NET Framework Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16937**	N/A	O-MIC-WIND-031120/1388
N/A	16-Oct-20	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	N/A	O-MIC-WIND-031120/1389

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unique from CVE-2020-16901. **CVE ID : CVE-2020-16938**		
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when Group Policy improperly checks access, aka 'Group Policy Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16939**	N/A	O-MIC-WIND-031120/1390
Improper Privilege Management	16-Oct-20	4.9	An elevation of privilege vulnerability exists when the Windows User Profile Service (ProfSvc) improperly handles junction points, aka 'Windows - User Profile Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16940**	N/A	O-MIC-WIND-031120/1391
Improper Release of Memory Before Removing Last Reference	16-Oct-20	5	A denial of service vulnerability exists in Microsoft Outlook software when the software fails to properly handle objects in memory, aka 'Microsoft Outlook Denial of Service Vulnerability'. **CVE ID : CVE-2020-16949**	N/A	O-MIC-WIND-031120/1392
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. This	N/A	O-MIC-WIND-031120/1393

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2020-16912, CVE-2020-16936, CVE-2020-16973, CVE-2020-16974, CVE-2020-16975, CVE-2020-16976. **CVE ID : CVE-2020-16972**		
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16912, CVE-2020-16936, CVE-2020-16972, CVE-2020-16974, CVE-2020-16975, CVE-2020-16976. **CVE ID : CVE-2020-16973**	N/A	O-MIC-WIND-031120/1394
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16912, CVE-2020-16936, CVE-2020-16972, CVE-2020-16973, CVE-2020-16975, CVE-2020-16976.	N/A	O-MIC-WIND-031120/1395

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-16974		
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16912, CVE-2020-16936, CVE-2020-16972, CVE-2020-16973, CVE-2020-16974, CVE-2020-16976. **CVE ID : CVE-2020-16975**	N/A	O-MIC-WIND-031120/1396
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16912, CVE-2020-16936, CVE-2020-16972, CVE-2020-16973, CVE-2020-16974, CVE-2020-16975. **CVE ID : CVE-2020-16976**	N/A	O-MIC-WIND-031120/1397
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows iSCSI Target Service improperly handles file operations, aka 'Windows	N/A	O-MIC-WIND-031120/1398

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			iSCSI Target Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16980**		
windows_server_2019					
Improper Privilege Management	16-Oct-20	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-2020-0764**	N/A	O-MIC-WIND-031120/1399
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Oct-20	7.2	An elevation of privilege vulnerability exists when Windows Hyper-V on a host server fails to properly handle objects in memory, aka 'Windows Hyper-V Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1080. **CVE ID : CVE-2020-1047**	N/A	O-MIC-WIND-031120/1400
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Oct-20	7.2	An elevation of privilege vulnerability exists when Windows Hyper-V on a host server fails to properly handle objects in memory, aka 'Windows Hyper-V Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-1047. **CVE ID : CVE-2020-1080**	N/A	O-MIC-WIND-031120/1401
Improper Restriction of Operations within the Bounds of a	16-Oct-20	9.3	A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components	N/A	O-MIC-WIND-031120/1402

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-16923. **CVE ID : CVE-2020-1167**		
N/A	16-Oct-20	4.6	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate specific malicious data from a user on a guest operating system.To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, running as a virtual machine, could run a specially crafted application.The security update addresses the vulnerability by resolving the conditions where Hyper-V would fail to handle these requests., aka 'Windows Hyper-V Denial of Service Vulnerability'. **CVE ID : CVE-2020-1243**	N/A	O-MIC-WIND-031120/1403
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Application Compatibility Client Library improperly handles registry operations, aka 'Windows Application Compatibility Client Library Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16920. **CVE ID : CVE-2020-16876**	N/A	O-MIC-WIND-031120/1404

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Storage VSP Driver improperly handles file operations, aka 'Windows Storage VSP Driver Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16885**	N/A	O-MIC-WIND-031120/1405
Improper Privilege Management	16-Oct-20	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'. **CVE ID : CVE-2020-16887**	N/A	O-MIC-WIND-031120/1406
Information Exposure	16-Oct-20	2.1	An information disclosure vulnerability exists when the Windows KernelStream improperly handles objects in memory, aka 'Windows KernelStream Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16889**	N/A	O-MIC-WIND-031120/1407
Improper Privilege Management	16-Oct-20	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16890**	N/A	O-MIC-WIND-031120/1408
Improper Input Validation	16-Oct-20	7.2	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an	N/A	O-MIC-WIND-031120/1409

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-16891**		
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists in the way that the Windows kernel image handles objects in memory.An attacker who successfully exploited the vulnerability could execute code with elevated permissions.To exploit the vulnerability, a locally authenticated attacker could run a specially crafted application.The security update addresses the vulnerability by ensuring the Windows kernel image properly handles objects in memory., aka 'Windows Image Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16892**	N/A	O-MIC-WIND-031120/1410
Improper Privilege Management	16-Oct-20	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-2020-16895**	N/A	O-MIC-WIND-031120/1411
Information Exposure	16-Oct-20	5	An information disclosure vulnerability exists in Remote Desktop Protocol (RDP)	N/A	O-MIC-WIND-031120/1412

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16896**		
N/A	16-Oct-20	2.1	An information disclosure vulnerability exists when NetBIOS over TCP (NBT) Extensions (NetBT) improperly handle objects in memory, aka 'NetBT Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16897**	N/A	O-MIC-WIND-031120/1413
N/A	16-Oct-20	5.8	A remote code execution vulnerability exists when the Windows TCP/IP stack improperly handles ICMPv6 Router Advertisement packets, aka 'Windows TCP/IP Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-16898**	N/A	O-MIC-WIND-031120/1414
N/A	16-Oct-20	7.8	A denial of service vulnerability exists when the Windows TCP/IP stack improperly handles ICMPv6 Router Advertisement packets, aka 'Windows TCP/IP Denial of Service Vulnerability'. **CVE ID : CVE-2020-16899**	N/A	O-MIC-WIND-031120/1415
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Event System improperly handles objects in	N/A	O-MIC-WIND-031120/1416

CVSS Scoring Scale	0-1	1-2	2-3	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.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Event System Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16900**		
Improper Privilege Management	16-Oct-20	7.2	An elevation of privilege vulnerability exists in the Windows Installer when the Windows Installer fails to properly sanitize input leading to an insecure library loading behavior.A locally authenticated attacker could run arbitrary code with elevated system privileges, aka 'Windows Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16902**	N/A	O-MIC-WIND-031120/1417
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16909. **CVE ID : CVE-2020-16905**	N/A	O-MIC-WIND-031120/1418
Improper Privilege Management	16-Oct-20	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k	N/A	O-MIC-WIND-031120/1419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16913. **CVE ID : CVE-2020-16907**		
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16905. **CVE ID : CVE-2020-16909**	N/A	O-MIC-WIND-031120/1420
Improper Preservation of Permissions	16-Oct-20	4.3	A security feature bypass vulnerability exists when Microsoft Windows fails to handle file creation permissions, which could allow an attacker to create files in a protected Unified Extensible Firmware Interface (UEFI) location.To exploit this vulnerability, an attacker could run a specially crafted application to bypass Unified Extensible Firmware Interface (UEFI) variable security in Windows.The security update addresses the vulnerability by correcting security feature behavior to enforce permissions., aka 'Windows Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-16910**	N/A	O-MIC-WIND-031120/1421
N/A	16-Oct-20	9.3	A remote code execution	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2020-16911**		031120/1422
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16936, CVE-2020-16972, CVE-2020-16973, CVE-2020-16974, CVE-2020-16975, CVE-2020-16976. **CVE ID : CVE-2020-16912**	N/A	O-MIC-WIND-031120/1423
Improper Privilege Management	16-Oct-20	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16907. **CVE ID : CVE-2020-16913**	N/A	O-MIC-WIND-031120/1424
Information Exposure	16-Oct-20	2.1	An information disclosure vulnerability exists in the way that the Windows	N/A	O-MIC-WIND-031120/1425

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Graphics Device Interface Plus (GDI+) handles objects in memory, allowing an attacker to retrieve information from a targeted system, aka 'Windows GDI+ Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16914**		
Out-of-bounds Write	16-Oct-20	6.8	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'. **CVE ID : CVE-2020-16915**	N/A	O-MIC-WIND-031120/1426
Improper Privilege Management	16-Oct-20	7.2	An elevation of privilege vulnerability exists when Windows improperly handles COM object creation, aka 'Windows COM Server Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16935. **CVE ID : CVE-2020-16916**	N/A	O-MIC-WIND-031120/1427
Information Exposure	16-Oct-20	2.1	An information disclosure vulnerability exists when the Windows Enterprise App Management Service improperly handles certain file operations, aka 'Windows Enterprise App Management Service Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16919**	N/A	O-MIC-WIND-031120/1428
Improper Privilege	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Windows Application Compatibility Client Library improperly handles registry operations, aka 'Windows Application Compatibility Client Library Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16876. **CVE ID : CVE-2020-16920**		031120/1429
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Oct-20	2.1	An information disclosure vulnerability exists in Text Services Framework when it fails to properly handle objects in memory, aka 'Windows Text Services Framework Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16921**	N/A	O-MIC-WIND-031120/1430
Improper Verification of Cryptographic Signature	16-Oct-20	2.1	A spoofing vulnerability exists when Windows incorrectly validates file signatures, aka 'Windows Spoofing Vulnerability'. **CVE ID : CVE-2020-16922**	N/A	O-MIC-WIND-031120/1431
N/A	16-Oct-20	6.8	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'. This CVE ID is unique from CVE-2020-1167. **CVE ID : CVE-2020-16923**	N/A	O-MIC-WIND-031120/1432
Improper Restriction of Operations	16-Oct-20	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in	N/A	O-MIC-WIND-031120/1433

CVSS Scoring Scale	0-1	1-2	2-3	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			memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2020-16924**		
N/A	16-Oct-20	7.8	A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability'. **CVE ID : CVE-2020-16927**	N/A	O-MIC-WIND-031120/1434
Improper Handling of Exceptional Conditions	16-Oct-20	6.8	A security feature bypass vulnerability exists in Microsoft Word software when it fails to properly handle .LNK files, aka 'Microsoft Word Security Feature Bypass Vulnerability'. **CVE ID : CVE-2020-16933**	N/A	O-MIC-WIND-031120/1435
Improper Privilege Management	16-Oct-20	7.2	An elevation of privilege vulnerability exists when Windows improperly handles COM object creation, aka 'Windows COM Server Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16916. **CVE ID : CVE-2020-16935**	N/A	O-MIC-WIND-031120/1436
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this	N/A	O-MIC-WIND-031120/1437

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 Backup Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16912, CVE-2020-16972, CVE-2020-16973, CVE-2020-16974, CVE-2020-16975, CVE-2020-16976. **CVE ID : CVE-2020-16936**		
Information Exposure	16-Oct-20	4.3	An information disclosure vulnerability exists when the .NET Framework improperly handles objects in memory, aka '.NET Framework Information Disclosure Vulnerability'. **CVE ID : CVE-2020-16937**	N/A	O-MIC-WIND-031120/1438
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when Group Policy improperly checks access, aka 'Group Policy Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16939**	N/A	O-MIC-WIND-031120/1439
Improper Privilege Management	16-Oct-20	4.9	An elevation of privilege vulnerability exists when the Windows User Profile Service (ProfSvc) improperly handles junction points, aka 'Windows - User Profile Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2020-16940**	N/A	O-MIC-WIND-031120/1440
Improper Release of Memory	16-Oct-20	5	A denial of service vulnerability exists in Microsoft Outlook software	N/A	O-MIC-WIND-031120/1441

CVSS Scoring Scale	0-1	1-2	2-3	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 Removing Last Reference			when the software fails to properly handle objects in memory, aka 'Microsoft Outlook Denial of Service Vulnerability'. **CVE ID : CVE-2020-16949**		
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16912, CVE-2020-16936, CVE-2020-16973, CVE-2020-16974, CVE-2020-16975, CVE-2020-16976. **CVE ID : CVE-2020-16972**	N/A	O-MIC-WIND-031120/1442
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16912, CVE-2020-16936, CVE-2020-16972, CVE-2020-16974, CVE-2020-16975, CVE-2020-16976.	N/A	O-MIC-WIND-031120/1443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-16973		
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16912, CVE-2020-16936, CVE-2020-16972, CVE-2020-16973, CVE-2020-16975, CVE-2020-16976. **CVE ID : CVE-2020-16974**	N/A	O-MIC-WIND-031120/1444
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16912, CVE-2020-16936, CVE-2020-16972, CVE-2020-16973, CVE-2020-16974, CVE-2020-16976. **CVE ID : CVE-2020-16975**	N/A	O-MIC-WIND-031120/1445
Improper Privilege Management	16-Oct-20	4.6	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations.To exploit this	N/A	O-MIC-WIND-031120/1446

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 Backup Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-16912, CVE-2020-16936, CVE-2020-16972, CVE-2020-16973, CVE-2020-16974, CVE-2020-16975. **CVE ID : CVE-2020-16976**		
Improper Privilege Management	16-Oct-20	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-2020-16980**	N/A	O-MIC-WIND-031120/1447
omniosce					
omnios					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	26-Oct-20	7.5	An issue was discovered in illumos before 2020-10-22, as used in OmniOS before r151030by, r151032ay, and r151034y and SmartOS before 20201022. There is a buffer overflow in parse_user_name in lib/libpam/pam_framework.c . **CVE ID : CVE-2020-27678**	N/A	O-OMN-OMNI-031120/1448
Opensuse					
leap					
N/A	22-Oct-20	7.5	Mozilla developers and community members reported memory safety bugs	N/A	O-OPE-LEAP-031120/1449

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			present in Firefox 81 and Firefox ESR 78.3. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox ESR < 78.4, Firefox < 82, and Thunderbird < 78.4. **CVE ID : CVE-2020-15683**		
N/A	16-Oct-20	5	An issue has been found in PowerDNS Recursor before 4.1.18, 4.2.x before 4.2.5, and 4.3.x before 4.3.5. A remote attacker can cause the cached records for a given name to be updated to the Bogus DNSSEC validation state, instead of their actual DNSSEC Secure state, via a DNS ANY query. This results in a denial of service for installation that always validate (dnssec=validate), and for clients requesting validation when on-demand validation is enabled (dnssec=process). **CVE ID : CVE-2020-25829**	https://docs.powerdns.com/recursor/security-advisories/powerdns-advisory-2020-07.html	O-OPE-LEAP-031120/1450
Oracle					
hospitality_res_3700_firmware					
N/A	21-Oct-20	5	Vulnerability in the Oracle Hospitality RES 3700 product of Oracle Food and Beverage Applications (component: CAL). The supported version that is affected is 5.7. Easily	N/A	O-ORA-HOSP-031120/1451

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitable vulnerability allows unauthenticated attacker with network access via TCP to compromise Oracle Hospitality RES 3700. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hospitality RES 3700 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-2020-14783**		
solaris					
N/A	21-Oct-20	10	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Pluggable authentication module). Supported versions that are affected are 10 and 11. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Solaris. While the vulnerability is in Oracle Solaris, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Solaris. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector:	N/A	O-ORA-SOLA-031120/1452

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2020-14871**		
N/A	21-Oct-20	4.9	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Filesystem). 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 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:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14754**	N/A	O-ORA-SOLA-031120/1453
N/A	21-Oct-20	3.6	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Kernel). 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	N/A	O-ORA-SOLA-031120/1454

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Solaris accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Solaris. CVSS 3.1 Base Score 5.6 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:L). **CVE ID : CVE-2020-14758**		
N/A	21-Oct-20	3.3	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Kernel). 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 and while the vulnerability is in Oracle Solaris, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Solaris accessible data. CVSS 3.1 Base Score 2.5	N/A	O-ORA-SOLA-031120/1455

CVSS Scoring Scale	0-1	1-2	2-3	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:L/AC:H/PR:L/UI:R/S:C/C:N/I:L/A:N). **CVE ID : CVE-2020-14759**		
N/A	21-Oct-20	2.1	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Utility). The supported version that is affected is 11. Difficult to exploit vulnerability allows low privileged attacker with network access via SSH 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 update, insert or delete access to some of Oracle Solaris accessible data. CVSS 3.1 Base Score 3.0 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:N/I:L/A:N). **CVE ID : CVE-2020-14818**	N/A	O-ORA-SOLA-031120/1456
Redhat					
enterprise_linux					
Allocation of Resources Without Limits or	20-Oct-20	5	A flaw was found in the way NSS handled CCS (ChangeCipherSpec) messages in TLS 1.3. This	N/A	O-RED-ENTE-031120/1457

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Throttling			flaw allows a remote attacker to send multiple CCS messages, causing a denial of service for servers compiled with the NSS library. The highest threat from this vulnerability is to system availability. This flaw affects NSS versions before 3.58. **CVE ID : CVE-2020-25648**		
Rockwellautomation					
flex_i\/o_1794-aent					
N/A	19-Oct-20	7.8	An exploitable denial of service vulnerability exists in the ENIP Request Path Logical Segment functionality of Allen-Bradley Flex IO 1794-AENT/B 4.003. A specially crafted network request can cause a loss of communications with the device resulting in denial-of-service. An attacker can send a malicious packet to trigger this vulnerability by sending an Electronic Key Segment with less bytes than required by the Key Format Table. **CVE ID : CVE-2020-6084**	N/A	O-ROC-FLEX-031120/1458
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-20	7.8	An exploitable denial of service vulnerability exists in the ENIP Request Path Logical Segment functionality of Allen-Bradley Flex IO 1794-AENT/B 4.003. A specially crafted network request can cause a loss of communications with the device resulting in denial-of-	N/A	O-ROC-FLEX-031120/1459

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service. An attacker can send a malicious packet to trigger this vulnerability by sending an Electronic Key Segment with less than 0x18 bytes following the Key Format field. **CVE ID : CVE-2020-6085**		
Sprecher-automation					
sprecon-e					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-Oct-20	7.2	Sprecher SPRECON-E firmware prior to 8.64b might allow local attackers with access to engineering data to insert arbitrary code. This firmware lacks the validation of the input values on the device side, which is provided by the engineering software during parameterization. Attackers with access to local configuration files can therefore insert malicious commands that are executed after compiling them to valid parameter files ("PDLs"), transferring them to the device, and restarting the device. **CVE ID : CVE-2020-11496**	https://www.sprecher-automation.com/en/it-security/	O-SPR-SPRE-031120/1460
Vmware					
esxi					
Time-of-check Time-of-use (TOCTOU) Race	20-Oct-20	3.5	VMware ESXi (7.0 before ESXi_7.0.1-0.0.16850804, 6.7 before ESXi670-202008101-SG, 6.5 before ESXi650-202007101-SG), Workstation (15.x), Fusion (11.x before	N/A	O-VMW-ESXI-031120/1461

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Condition			11.5.6) contain an out-of-bounds read vulnerability due to a time-of-check time-of-use issue in ACPI device. A malicious actor with administrative access to a virtual machine may be able to exploit this issue to leak memory from the vmx process. **CVE ID : CVE-2020-3981**		
Out-of-bounds Write	20-Oct-20	4.9	VMware ESXi (7.0 before ESXi_7.0.1-0.0.16850804, 6.7 before ESXi670-202008101-SG, 6.5 before ESXi650-202007101-SG), Workstation (15.x), Fusion (11.x before 11.5.6) contain an out-of-bounds write vulnerability due to a time-of-check time-of-use issue in ACPI device. A malicious actor with administrative access to a virtual machine may be able to exploit this vulnerability to crash the virtual machine's vmx process or corrupt hypervisor's memory heap. **CVE ID : CVE-2020-3982**	N/A	O-VMW-ESXI-031120/1462
Use After Free	20-Oct-20	10	OpenSLP as used in VMware ESXi (7.0 before ESXi_7.0.1-0.0.16850804, 6.7 before ESXi670-202010401-SG, 6.5 before ESXi650-202010401-SG) has a use-after-free issue. A malicious actor residing in the management network who has access to port 427 on an ESXi machine may be able to trigger a use-after-	N/A	O-VMW-ESXI-031120/1463

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			free in the OpenSLP service resulting in remote code execution. **CVE ID : CVE-2020-3992**		
Improper Release of Memory Before Removing Last Reference	20-Oct-20	3.5	In VMware ESXi (6.7 before ESXi670-201908101-SG, 6.5 before ESXi650-202007101-SG), Workstation (15.x before 15.1.0), Fusion (11.x before 11.1.0), the VMCI host drivers used by VMware hypervisors contain a memory leak vulnerability. A malicious actor with access to a virtual machine may be able to trigger a memory leak issue resulting in memory resource exhaustion on the hypervisor if the attack is sustained for extended periods of time. **CVE ID : CVE-2020-3995**	N/A	O-VMW-ESXI-031120/1464
XEN					
xen					
Insufficient Verification of Data Authenticity	22-Oct-20	7.2	An issue was discovered in Xen through 4.14.x allowing x86 guest OS users to cause a denial of service (data corruption), cause a data leak, or possibly gain privileges because an AMD IOMMU page-table entry can be half-updated. **CVE ID : CVE-2020-27670**	N/A	O-XEN-XEN-031120/1465
Improper Privilege Management	22-Oct-20	7.2	An issue was discovered in Xen through 4.14.x allowing x86 HVM and PVH guest OS users to cause a denial of service (data corruption), cause a data leak, or possibly	N/A	O-XEN-XEN-031120/1466

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			gain privileges because coalescing of per-page IOMMU TLB flushes is mishandled. **CVE ID : CVE-2020-27671**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-Oct-20	6.9	An issue was discovered in Xen through 4.14.x allowing x86 guest OS users to cause a host OS denial of service, achieve data corruption, or possibly gain privileges by exploiting a race condition that leads to a use-after-free involving 2MiB and 1GiB superpages. **CVE ID : CVE-2020-27672**	N/A	O-XEN-XEN-031120/1467
Uncontrolled Resource Consumption	22-Oct-20	4.9	An issue was discovered in the Linux kernel through 5.9.1, as used with Xen through 4.14.x. Guest OS users can cause a denial of service (host OS hang) via a high rate of events to dom0, aka CID-e99502f76271. **CVE ID : CVE-2020-27673**	N/A	O-XEN-XEN-031120/1468
Hardware					
Belkin					
linksys_wrt_160nl					
Out-of-bounds Write	23-Oct-20	6.5	** UNSUPPORTED WHEN ASSIGNED ** Belkin LINKSYS WRT160NL 1.0.04.002_US_20130619 devices have a stack-based buffer overflow vulnerability because of sprintf in create_dir in mini_httpd. Successful exploitation leads to arbitrary code execution.	N/A	H-BEL-LINK-031120/1469

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2020-26561**		
Cisco					
isr_4431					
N/A	21-Oct-20	5	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured File Policy for HTTP. The vulnerability is due to incorrect detection of modified HTTP packets used in chunked responses. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass a configured File Policy for HTTP packets and deliver a malicious payload. **CVE ID : CVE-2020-3299**	N/A	H-CIS-ISR_-031120/1470
isr_4461					
N/A	21-Oct-20	5	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured File Policy for HTTP. The vulnerability is due to incorrect detection of modified HTTP packets used	N/A	H-CIS-ISR_-031120/1471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in chunked responses. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass a configured File Policy for HTTP packets and deliver a malicious payload. **CVE ID : CVE-2020-3299**		
meraki_mx					
N/A	21-Oct-20	5	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured File Policy for HTTP. The vulnerability is due to incorrect detection of modified HTTP packets used in chunked responses. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass a configured File Policy for HTTP packets and deliver a malicious payload. **CVE ID : CVE-2020-3299**	N/A	H-CIS-MERA-031120/1472
1100-4p					
N/A	21-Oct-20	5	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote	N/A	H-CIS-1100-031120/1473

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to bypass a configured File Policy for HTTP. The vulnerability is due to incorrect detection of modified HTTP packets used in chunked responses. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass a configured File Policy for HTTP packets and deliver a malicious payload. **CVE ID : CVE-2020-3299**		
1100-8p					
N/A	21-Oct-20	5	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured File Policy for HTTP. The vulnerability is due to incorrect detection of modified HTTP packets used in chunked responses. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass a configured File Policy for HTTP packets and deliver a malicious payload. **CVE ID : CVE-2020-3299**	N/A	H-CIS-1100-031120/1474
1101-4p					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	21-Oct-20	5	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured File Policy for HTTP. The vulnerability is due to incorrect detection of modified HTTP packets used in chunked responses. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass a configured File Policy for HTTP packets and deliver a malicious payload. **CVE ID : CVE-2020-3299**	N/A	H-CIS-1101-031120/1475
1109-2p					
N/A	21-Oct-20	5	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured File Policy for HTTP. The vulnerability is due to incorrect detection of modified HTTP packets used in chunked responses. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass a configured File Policy for	N/A	H-CIS-1109-031120/1476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HTTP packets and deliver a malicious payload. **CVE ID : CVE-2020-3299**		
1109-4p					
N/A	21-Oct-20	5	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured File Policy for HTTP. The vulnerability is due to incorrect detection of modified HTTP packets used in chunked responses. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass a configured File Policy for HTTP packets and deliver a malicious payload. **CVE ID : CVE-2020-3299**	N/A	H-CIS-1109-031120/1477
1111x-8p					
N/A	21-Oct-20	5	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured File Policy for HTTP. The vulnerability is due to incorrect detection of modified HTTP packets used in chunked responses. An attacker could exploit this vulnerability by sending	N/A	H-CIS-1111-031120/1478

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass a configured File Policy for HTTP packets and deliver a malicious payload. **CVE ID : CVE-2020-3299**		
isr_4221					
N/A	21-Oct-20	5	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured File Policy for HTTP. The vulnerability is due to incorrect detection of modified HTTP packets used in chunked responses. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass a configured File Policy for HTTP packets and deliver a malicious payload. **CVE ID : CVE-2020-3299**	N/A	H-CIS-ISR_-031120/1479
isr_4331					
N/A	21-Oct-20	5	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured File Policy for HTTP. The vulnerability is	N/A	H-CIS-ISR_-031120/1480

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			due to incorrect detection of modified HTTP packets used in chunked responses. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass a configured File Policy for HTTP packets and deliver a malicious payload. **CVE ID : CVE-2020-3299**		
firepower_4115					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3457**	N/A	H-CIS-FIRE-031120/1481
Improper Neutralization of Special Elements used in an OS Command	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The	N/A	H-CIS-FIRE-031120/1482

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3459**		
N/A	21-Oct-20	7.2	A vulnerability in the secure boot process of Cisco FXOS Software could allow an authenticated, local attacker to bypass the secure boot mechanisms. The vulnerability is due to insufficient protections of the secure boot process. An attacker could exploit this vulnerability by injecting code into a specific file that is then referenced during the device boot process. A successful exploit could allow the attacker to break the chain of trust and inject code into the boot process of the device which would be executed at each boot and maintain persistence across reboots. **CVE ID : CVE-2020-3455**	N/A	H-CIS-FIRE-031120/1483
Cross-Site Request Forgery	21-Oct-20	6.8	A vulnerability in the Cisco Firepower Chassis Manager (FCM) of Cisco FXOS Software	N/A	H-CIS-FIRE-031120/1484

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(CSRF)			could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of an affected device. The vulnerability is due to insufficient CSRF protections for the FCM interface. An attacker could exploit this vulnerability by persuading a targeted user to click a malicious link. A successful exploit could allow the attacker to send arbitrary requests that could take unauthorized actions on behalf of the targeted user. **CVE ID : CVE-2020-3456**		
Improper Input Validation	21-Oct-20	7.8	A vulnerability in the ICMP ingress packet processing of Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 4110 appliances could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to incomplete input validation upon receiving ICMP packets. An attacker could exploit this vulnerability by sending a high number of crafted ICMP or ICMPv6 packets to an affected device. A successful exploit could allow the attacker to cause a memory exhaustion condition that may result in an unexpected	N/A	H-CIS-FIRE-031120/1485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reload. No manual intervention is needed to recover the device after the reload. **CVE ID : CVE-2020-3571**		
firepower_4125					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3457**	N/A	H-CIS-FIRE-031120/1486
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A	N/A	H-CIS-FIRE-031120/1487

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3459**		
N/A	21-Oct-20	7.2	A vulnerability in the secure boot process of Cisco FXOS Software could allow an authenticated, local attacker to bypass the secure boot mechanisms. The vulnerability is due to insufficient protections of the secure boot process. An attacker could exploit this vulnerability by injecting code into a specific file that is then referenced during the device boot process. A successful exploit could allow the attacker to break the chain of trust and inject code into the boot process of the device which would be executed at each boot and maintain persistence across reboots. **CVE ID : CVE-2020-3455**	N/A	H-CIS-FIRE-031120/1488
Cross-Site Request Forgery (CSRF)	21-Oct-20	6.8	A vulnerability in the Cisco Firepower Chassis Manager (FCM) of Cisco FXOS Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of an affected device. The vulnerability is due to insufficient CSRF protections	N/A	H-CIS-FIRE-031120/1489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for the FCM interface. An attacker could exploit this vulnerability by persuading a targeted user to click a malicious link. A successful exploit could allow the attacker to send arbitrary requests that could take unauthorized actions on behalf of the targeted user. **CVE ID : CVE-2020-3456**		
Improper Input Validation	21-Oct-20	7.8	A vulnerability in the ICMP ingress packet processing of Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 4110 appliances could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to incomplete input validation upon receiving ICMP packets. An attacker could exploit this vulnerability by sending a high number of crafted ICMP or ICMPv6 packets to an affected device. A successful exploit could allow the attacker to cause a memory exhaustion condition that may result in an unexpected reload. No manual intervention is needed to recover the device after the reload. **CVE ID : CVE-2020-3571**	N/A	H-CIS-FIRE-031120/1490
firepower_4145					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3457**	N/A	H-CIS-FIRE-031120/1491
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3459**	N/A	H-CIS-FIRE-031120/1492

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	21-Oct-20	7.2	A vulnerability in the secure boot process of Cisco FXOS Software could allow an authenticated, local attacker to bypass the secure boot mechanisms. The vulnerability is due to insufficient protections of the secure boot process. An attacker could exploit this vulnerability by injecting code into a specific file that is then referenced during the device boot process. A successful exploit could allow the attacker to break the chain of trust and inject code into the boot process of the device which would be executed at each boot and maintain persistence across reboots. **CVE ID : CVE-2020-3455**	N/A	H-CIS-FIRE-031120/1493
Cross-Site Request Forgery (CSRF)	21-Oct-20	6.8	A vulnerability in the Cisco Firepower Chassis Manager (FCM) of Cisco FXOS Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of an affected device. The vulnerability is due to insufficient CSRF protections for the FCM interface. An attacker could exploit this vulnerability by persuading a targeted user to click a malicious link. A successful exploit could allow the attacker to send arbitrary	N/A	H-CIS-FIRE-031120/1494

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			requests that could take unauthorized actions on behalf of the targeted user. **CVE ID : CVE-2020-3456**		
Improper Input Validation	21-Oct-20	7.8	A vulnerability in the ICMP ingress packet processing of Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 4110 appliances could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to incomplete input validation upon receiving ICMP packets. An attacker could exploit this vulnerability by sending a high number of crafted ICMP or ICMPv6 packets to an affected device. A successful exploit could allow the attacker to cause a memory exhaustion condition that may result in an unexpected reload. No manual intervention is needed to recover the device after the reload. **CVE ID : CVE-2020-3571**	N/A	H-CIS-FIRE-031120/1495
firepower_4110					
Improper Neutralization of Special Elements used in an OS Command ('OS Command	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation	N/A	H-CIS-FIRE-031120/1496

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3457**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3459**	N/A	H-CIS-FIRE-031120/1497
N/A	21-Oct-20	7.2	A vulnerability in the secure boot process of Cisco FXOS Software could allow an authenticated, local attacker to bypass the secure boot mechanisms. The vulnerability is due to insufficient protections of the	N/A	H-CIS-FIRE-031120/1498

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			secure boot process. An attacker could exploit this vulnerability by injecting code into a specific file that is then referenced during the device boot process. A successful exploit could allow the attacker to break the chain of trust and inject code into the boot process of the device which would be executed at each boot and maintain persistence across reboots. **CVE ID : CVE-2020-3455**		
Cross-Site Request Forgery (CSRF)	21-Oct-20	6.8	A vulnerability in the Cisco Firepower Chassis Manager (FCM) of Cisco FXOS Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of an affected device. The vulnerability is due to insufficient CSRF protections for the FCM interface. An attacker could exploit this vulnerability by persuading a targeted user to click a malicious link. A successful exploit could allow the attacker to send arbitrary requests that could take unauthorized actions on behalf of the targeted user. **CVE ID : CVE-2020-3456**	N/A	H-CIS-FIRE-031120/1499
Improper Input Validation	21-Oct-20	7.8	A vulnerability in the ICMP ingress packet processing of Cisco Firepower Threat	N/A	H-CIS-FIRE-031120/1500

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Defense (FTD) Software for Cisco Firepower 4110 appliances could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to incomplete input validation upon receiving ICMP packets. An attacker could exploit this vulnerability by sending a high number of crafted ICMP or ICMPv6 packets to an affected device. A successful exploit could allow the attacker to cause a memory exhaustion condition that may result in an unexpected reload. No manual intervention is needed to recover the device after the reload. **CVE ID : CVE-2020-3571**		
firepower_4120					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow	N/A	H-CIS-FIRE-031120/1501

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3457**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3459**	N/A	H-CIS-FIRE-031120/1502
N/A	21-Oct-20	7.2	A vulnerability in the secure boot process of Cisco FXOS Software could allow an authenticated, local attacker to bypass the secure boot mechanisms. The vulnerability is due to insufficient protections of the secure boot process. An attacker could exploit this vulnerability by injecting code into a specific file that is then referenced during the device boot process. A successful exploit could allow	N/A	H-CIS-FIRE-031120/1503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the attacker to break the chain of trust and inject code into the boot process of the device which would be executed at each boot and maintain persistence across reboots. **CVE ID : CVE-2020-3455**		
Cross-Site Request Forgery (CSRF)	21-Oct-20	6.8	A vulnerability in the Cisco Firepower Chassis Manager (FCM) of Cisco FXOS Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of an affected device. The vulnerability is due to insufficient CSRF protections for the FCM interface. An attacker could exploit this vulnerability by persuading a targeted user to click a malicious link. A successful exploit could allow the attacker to send arbitrary requests that could take unauthorized actions on behalf of the targeted user. **CVE ID : CVE-2020-3456**	N/A	H-CIS-FIRE-031120/1504
Improper Input Validation	21-Oct-20	7.8	A vulnerability in the ICMP ingress packet processing of Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 4110 appliances could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The	N/A	H-CIS-FIRE-031120/1505

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to incomplete input validation upon receiving ICMP packets. An attacker could exploit this vulnerability by sending a high number of crafted ICMP or ICMPv6 packets to an affected device. A successful exploit could allow the attacker to cause a memory exhaustion condition that may result in an unexpected reload. No manual intervention is needed to recover the device after the reload. **CVE ID : CVE-2020-3571**		
firepower_4140					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3457**	N/A	H-CIS-FIRE-031120/1506
Improper Neutralizatio	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could	N/A	H-CIS-FIRE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in an OS Command ('OS Command Injection')			allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3459**		031120/1507
N/A	21-Oct-20	7.2	A vulnerability in the secure boot process of Cisco FXOS Software could allow an authenticated, local attacker to bypass the secure boot mechanisms. The vulnerability is due to insufficient protections of the secure boot process. An attacker could exploit this vulnerability by injecting code into a specific file that is then referenced during the device boot process. A successful exploit could allow the attacker to break the chain of trust and inject code into the boot process of the device which would be executed at each boot and maintain persistence across reboots.	N/A	H-CIS-FIRE-031120/1508

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3455		
Cross-Site Request Forgery (CSRF)	21-Oct-20	6.8	A vulnerability in the Cisco Firepower Chassis Manager (FCM) of Cisco FXOS Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of an affected device. The vulnerability is due to insufficient CSRF protections for the FCM interface. An attacker could exploit this vulnerability by persuading a targeted user to click a malicious link. A successful exploit could allow the attacker to send arbitrary requests that could take unauthorized actions on behalf of the targeted user. **CVE ID : CVE-2020-3456**	N/A	H-CIS-FIRE-031120/1509
Improper Input Validation	21-Oct-20	7.8	A vulnerability in the ICMP ingress packet processing of Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 4110 appliances could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to incomplete input validation upon receiving ICMP packets. An attacker could exploit this vulnerability by sending a high number of crafted ICMP or ICMPv6 packets to an	N/A	H-CIS-FIRE-031120/1510

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to cause a memory exhaustion condition that may result in an unexpected reload. No manual intervention is needed to recover the device after the reload. **CVE ID : CVE-2020-3571**		
firepower_4150					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3457**	N/A	H-CIS-FIRE-031120/1511
Improper Neutralization of Special Elements used in an OS Command ('OS Command	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the	N/A	H-CIS-FIRE-031120/1512

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3459**		
N/A	21-Oct-20	7.2	A vulnerability in the secure boot process of Cisco FXOS Software could allow an authenticated, local attacker to bypass the secure boot mechanisms. The vulnerability is due to insufficient protections of the secure boot process. An attacker could exploit this vulnerability by injecting code into a specific file that is then referenced during the device boot process. A successful exploit could allow the attacker to break the chain of trust and inject code into the boot process of the device which would be executed at each boot and maintain persistence across reboots. **CVE ID : CVE-2020-3455**	N/A	H-CIS-FIRE-031120/1513
Cross-Site Request Forgery (CSRF)	21-Oct-20	6.8	A vulnerability in the Cisco Firepower Chassis Manager (FCM) of Cisco FXOS Software could allow an unauthenticated, remote attacker to conduct a cross-	N/A	H-CIS-FIRE-031120/1514

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			site request forgery (CSRF) attack against a user of an affected device. The vulnerability is due to insufficient CSRF protections for the FCM interface. An attacker could exploit this vulnerability by persuading a targeted user to click a malicious link. A successful exploit could allow the attacker to send arbitrary requests that could take unauthorized actions on behalf of the targeted user. **CVE ID : CVE-2020-3456**		
Improper Input Validation	21-Oct-20	7.8	A vulnerability in the ICMP ingress packet processing of Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 4110 appliances could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to incomplete input validation upon receiving ICMP packets. An attacker could exploit this vulnerability by sending a high number of crafted ICMP or ICMPv6 packets to an affected device. A successful exploit could allow the attacker to cause a memory exhaustion condition that may result in an unexpected reload. No manual intervention is needed to recover the device after the	N/A	H-CIS-FIRE-031120/1515

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reload. **CVE ID : CVE-2020-3571**		
firepower_1010					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3457**	N/A	H-CIS-FIRE-031120/1516
N/A	21-Oct-20	4.6	Multiple vulnerabilities in the secure boot process of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software for the Firepower 1000 Series and Firepower 2100 Series Appliances could allow an authenticated, local attacker to bypass the secure boot mechanism. The vulnerabilities are due to insufficient protections of the secure boot process. An attacker could exploit these vulnerabilities by injecting	N/A	H-CIS-FIRE-031120/1517

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code into specific files that are then referenced during the device boot process. A successful exploit could allow the attacker to break the chain of trust and inject code into the boot process of the device, which would be executed at each boot and maintain persistence across reboots. **CVE ID : CVE-2020-3458**		
Information Exposure Through Discrepancy	21-Oct-20	4.3	A vulnerability in the TLS handler of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 1000 Series firewalls could allow an unauthenticated, remote attacker to gain access to sensitive information. The vulnerability is due to improper implementation of countermeasures against the Bleichenbacher attack for cipher suites that rely on RSA for key exchange. An attacker could exploit this vulnerability by sending crafted TLS messages to the device, which would act as an oracle and allow the attacker to carry out a chosen-ciphertext attack. A successful exploit could allow the attacker to perform cryptanalytic operations that may allow decryption of previously captured TLS	N/A	H-CIS-FIRE-031120/1518

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sessions to the affected device. To exploit this vulnerability, an attacker must be able to perform both of the following actions: Capture TLS traffic that is in transit between clients and the affected device Actively establish a considerable number of TLS connections to the affected device **CVE ID : CVE-2020-3585**		
firepower_1120					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3457**	N/A	H-CIS-FIRE-031120/1519
N/A	21-Oct-20	4.6	Multiple vulnerabilities in the secure boot process of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software for the Firepower 1000 Series and	N/A	H-CIS-FIRE-031120/1520

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Firepower 2100 Series Appliances could allow an authenticated, local attacker to bypass the secure boot mechanism. The vulnerabilities are due to insufficient protections of the secure boot process. An attacker could exploit these vulnerabilities by injecting code into specific files that are then referenced during the device boot process. A successful exploit could allow the attacker to break the chain of trust and inject code into the boot process of the device, which would be executed at each boot and maintain persistence across reboots. **CVE ID : CVE-2020-3458**		
Information Exposure Through Discrepancy	21-Oct-20	4.3	A vulnerability in the TLS handler of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 1000 Series firewalls could allow an unauthenticated, remote attacker to gain access to sensitive information. The vulnerability is due to improper implementation of countermeasures against the Bleichenbacher attack for cipher suites that rely on RSA for key exchange. An attacker could exploit this vulnerability by sending	N/A	H-CIS-FIRE-031120/1521

CVSS Scoring Scale	0-1	1-2	2-3	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 TLS messages to the device, which would act as an oracle and allow the attacker to carry out a chosen-ciphertext attack. A successful exploit could allow the attacker to perform cryptanalytic operations that may allow decryption of previously captured TLS sessions to the affected device. To exploit this vulnerability, an attacker must be able to perform both of the following actions: Capture TLS traffic that is in transit between clients and the affected device Actively establish a considerable number of TLS connections to the affected device **CVE ID : CVE-2020-3585**		
firepower_1140					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying	N/A	H-CIS-FIRE-031120/1522

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating system with root privileges. **CVE ID : CVE-2020-3457**		
N/A	21-Oct-20	4.6	Multiple vulnerabilities in the secure boot process of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software for the Firepower 1000 Series and Firepower 2100 Series Appliances could allow an authenticated, local attacker to bypass the secure boot mechanism. The vulnerabilities are due to insufficient protections of the secure boot process. An attacker could exploit these vulnerabilities by injecting code into specific files that are then referenced during the device boot process. A successful exploit could allow the attacker to break the chain of trust and inject code into the boot process of the device, which would be executed at each boot and maintain persistence across reboots. **CVE ID : CVE-2020-3458**	N/A	H-CIS-FIRE-031120/1523
Information Exposure Through Discrepancy	21-Oct-20	4.3	A vulnerability in the TLS handler of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 1000 Series firewalls could allow an	N/A	H-CIS-FIRE-031120/1524

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to gain access to sensitive information. The vulnerability is due to improper implementation of countermeasures against the Bleichenbacher attack for cipher suites that rely on RSA for key exchange. An attacker could exploit this vulnerability by sending crafted TLS messages to the device, which would act as an oracle and allow the attacker to carry out a chosen-ciphertext attack. A successful exploit could allow the attacker to perform cryptanalytic operations that may allow decryption of previously captured TLS sessions to the affected device. To exploit this vulnerability, an attacker must be able to perform both of the following actions: Capture TLS traffic that is in transit between clients and the affected device Actively establish a considerable number of TLS connections to the affected device **CVE ID : CVE-2020-3585**		
firepower_2110					
Improper Neutralization of Special Elements used in an OS Command	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The	N/A	H-CIS-FIRE-031120/1525

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3457**		
N/A	21-Oct-20	4.6	Multiple vulnerabilities in the secure boot process of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software for the Firepower 1000 Series and Firepower 2100 Series Appliances could allow an authenticated, local attacker to bypass the secure boot mechanism. The vulnerabilities are due to insufficient protections of the secure boot process. An attacker could exploit these vulnerabilities by injecting code into specific files that are then referenced during the device boot process. A successful exploit could allow the attacker to break the chain of trust and inject code into the boot process of the device, which would be executed at each boot and maintain persistence across	N/A	H-CIS-FIRE-031120/1526

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reboots. **CVE ID : CVE-2020-3458**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-Oct-20	7.1	A vulnerability in the SSL/TLS inspection of Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 2100 Series firewalls could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper input validation for certain fields of specific SSL/TLS messages. An attacker could exploit this vulnerability by sending a malformed SSL/TLS message through an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. No manual intervention is needed to recover the device after it has reloaded. **CVE ID : CVE-2020-3562**	N/A	H-CIS-FIRE-031120/1527
firepower_2120					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by	N/A	H-CIS-FIRE-031120/1528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3457**		
N/A	21-Oct-20	4.6	Multiple vulnerabilities in the secure boot process of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software for the Firepower 1000 Series and Firepower 2100 Series Appliances could allow an authenticated, local attacker to bypass the secure boot mechanism. The vulnerabilities are due to insufficient protections of the secure boot process. An attacker could exploit these vulnerabilities by injecting code into specific files that are then referenced during the device boot process. A successful exploit could allow the attacker to break the chain of trust and inject code into the boot process of the device, which would be executed at each boot and maintain persistence across reboots. **CVE ID : CVE-2020-3458**	N/A	H-CIS-FIRE-031120/1529
Improper Restriction	21-Oct-20	7.1	A vulnerability in the SSL/TLS inspection of Cisco	N/A	H-CIS-FIRE-031120/1530

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			Firepower Threat Defense (FTD) Software for Cisco Firepower 2100 Series firewalls could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper input validation for certain fields of specific SSL/TLS messages. An attacker could exploit this vulnerability by sending a malformed SSL/TLS message through an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. No manual intervention is needed to recover the device after it has reloaded. **CVE ID : CVE-2020-3562**		
firepower_2130					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow	N/A	H-CIS-FIRE-031120/1531

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3457**		
N/A	21-Oct-20	4.6	Multiple vulnerabilities in the secure boot process of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software for the Firepower 1000 Series and Firepower 2100 Series Appliances could allow an authenticated, local attacker to bypass the secure boot mechanism. The vulnerabilities are due to insufficient protections of the secure boot process. An attacker could exploit these vulnerabilities by injecting code into specific files that are then referenced during the device boot process. A successful exploit could allow the attacker to break the chain of trust and inject code into the boot process of the device, which would be executed at each boot and maintain persistence across reboots. **CVE ID : CVE-2020-3458**	N/A	H-CIS-FIRE-031120/1532
Improper Restriction of Operations within the Bounds of a	21-Oct-20	7.1	A vulnerability in the SSL/TLS inspection of Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 2100 Series firewalls could allow an	N/A	H-CIS-FIRE-031120/1533

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper input validation for certain fields of specific SSL/TLS messages. An attacker could exploit this vulnerability by sending a malformed SSL/TLS message through an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. No manual intervention is needed to recover the device after it has reloaded. **CVE ID : CVE-2020-3562**		
firepower_2140					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges.	N/A	H-CIS-FIRE-031120/1534

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3457		
N/A	21-Oct-20	4.6	Multiple vulnerabilities in the secure boot process of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software for the Firepower 1000 Series and Firepower 2100 Series Appliances could allow an authenticated, local attacker to bypass the secure boot mechanism. The vulnerabilities are due to insufficient protections of the secure boot process. An attacker could exploit these vulnerabilities by injecting code into specific files that are then referenced during the device boot process. A successful exploit could allow the attacker to break the chain of trust and inject code into the boot process of the device, which would be executed at each boot and maintain persistence across reboots. **CVE ID : CVE-2020-3458**	N/A	H-CIS-FIRE-031120/1535
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-Oct-20	7.1	A vulnerability in the SSL/TLS inspection of Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 2100 Series firewalls could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The	N/A	H-CIS-FIRE-031120/1536

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to improper input validation for certain fields of specific SSL/TLS messages. An attacker could exploit this vulnerability by sending a malformed SSL/TLS message through an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. No manual intervention is needed to recover the device after it has reloaded. **CVE ID : CVE-2020-3562**		
isa_3000					
N/A	21-Oct-20	5	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured File Policy for HTTP. The vulnerability is due to incorrect detection of modified HTTP packets used in chunked responses. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass a configured File Policy for HTTP packets and deliver a malicious payload. **CVE ID : CVE-2020-3299**	N/A	H-CIS-ISA_-031120/1537
firepower_1000					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3457**	N/A	H-CIS-FIRE-031120/1538
Information Exposure Through Discrepancy	21-Oct-20	4.3	A vulnerability in the TLS handler of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 1000 Series firewalls could allow an unauthenticated, remote attacker to gain access to sensitive information. The vulnerability is due to improper implementation of countermeasures against the Bleichenbacher attack for cipher suites that rely on RSA for key exchange. An attacker could exploit this vulnerability by sending crafted TLS messages to the device, which would act as an	N/A	H-CIS-FIRE-031120/1539

CVSS Scoring Scale	0-1	1-2	2-3	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 and allow the attacker to carry out a chosen-ciphertext attack. A successful exploit could allow the attacker to perform cryptanalytic operations that may allow decryption of previously captured TLS sessions to the affected device. To exploit this vulnerability, an attacker must be able to perform both of the following actions: Capture TLS traffic that is in transit between clients and the affected device Actively establish a considerable number of TLS connections to the affected device **CVE ID : CVE-2020-3585**		
firepower_2100					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges.	N/A	H-CIS-FIRE-031120/1540

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3457		
firepower_4112					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3457**	N/A	H-CIS-FIRE-031120/1541
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root	N/A	H-CIS-FIRE-031120/1542

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges. **CVE ID : CVE-2020-3459**		
N/A	21-Oct-20	7.2	A vulnerability in the secure boot process of Cisco FXOS Software could allow an authenticated, local attacker to bypass the secure boot mechanisms. The vulnerability is due to insufficient protections of the secure boot process. An attacker could exploit this vulnerability by injecting code into a specific file that is then referenced during the device boot process. A successful exploit could allow the attacker to break the chain of trust and inject code into the boot process of the device which would be executed at each boot and maintain persistence across reboots. **CVE ID : CVE-2020-3455**	N/A	H-CIS-FIRE-031120/1543
Cross-Site Request Forgery (CSRF)	21-Oct-20	6.8	A vulnerability in the Cisco Firepower Chassis Manager (FCM) of Cisco FXOS Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of an affected device. The vulnerability is due to insufficient CSRF protections for the FCM interface. An attacker could exploit this vulnerability by persuading a targeted user to click a	N/A	H-CIS-FIRE-031120/1544

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious link. A successful exploit could allow the attacker to send arbitrary requests that could take unauthorized actions on behalf of the targeted user. **CVE ID : CVE-2020-3456**		
Improper Input Validation	21-Oct-20	7.8	A vulnerability in the ICMP ingress packet processing of Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 4110 appliances could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to incomplete input validation upon receiving ICMP packets. An attacker could exploit this vulnerability by sending a high number of crafted ICMP or ICMPv6 packets to an affected device. A successful exploit could allow the attacker to cause a memory exhaustion condition that may result in an unexpected reload. No manual intervention is needed to recover the device after the reload. **CVE ID : CVE-2020-3571**	N/A	H-CIS-FIRE-031120/1545
firepower_1150					
Improper Neutralization of Special Elements used in an OS	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed	N/A	H-CIS-FIRE-031120/1546

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3457**		
N/A	21-Oct-20	4.6	Multiple vulnerabilities in the secure boot process of Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software for the Firepower 1000 Series and Firepower 2100 Series Appliances could allow an authenticated, local attacker to bypass the secure boot mechanism. The vulnerabilities are due to insufficient protections of the secure boot process. An attacker could exploit these vulnerabilities by injecting code into specific files that are then referenced during the device boot process. A successful exploit could allow the attacker to break the chain of trust and inject code into the boot process of the device, which would be executed at each boot and	N/A	H-CIS-FIRE-031120/1547

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			maintain persistence across reboots. **CVE ID : CVE-2020-3458**		
Information Exposure Through Discrepancy	21-Oct-20	4.3	A vulnerability in the TLS handler of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 1000 Series firewalls could allow an unauthenticated, remote attacker to gain access to sensitive information. The vulnerability is due to improper implementation of countermeasures against the Bleichenbacher attack for cipher suites that rely on RSA for key exchange. An attacker could exploit this vulnerability by sending crafted TLS messages to the device, which would act as an oracle and allow the attacker to carry out a chosen-ciphertext attack. A successful exploit could allow the attacker to perform cryptanalytic operations that may allow decryption of previously captured TLS sessions to the affected device. To exploit this vulnerability, an attacker must be able to perform both of the following actions: Capture TLS traffic that is in transit between clients and the affected device Actively establish a considerable	N/A	H-CIS-FIRE-031120/1548

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			number of TLS connections to the affected device **CVE ID : CVE-2020-3585**		
firepower_9300_sm-24					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3457**	N/A	H-CIS-FIRE-031120/1549
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute	N/A	H-CIS-FIRE-031120/1550

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3459**		
N/A	21-Oct-20	7.2	A vulnerability in the secure boot process of Cisco FXOS Software could allow an authenticated, local attacker to bypass the secure boot mechanisms. The vulnerability is due to insufficient protections of the secure boot process. An attacker could exploit this vulnerability by injecting code into a specific file that is then referenced during the device boot process. A successful exploit could allow the attacker to break the chain of trust and inject code into the boot process of the device which would be executed at each boot and maintain persistence across reboots. **CVE ID : CVE-2020-3455**	N/A	H-CIS-FIRE-031120/1551
Cross-Site Request Forgery (CSRF)	21-Oct-20	6.8	A vulnerability in the Cisco Firepower Chassis Manager (FCM) of Cisco FXOS Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of an affected device. The vulnerability is due to insufficient CSRF protections for the FCM interface. An attacker could exploit this	N/A	H-CIS-FIRE-031120/1552

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by persuading a targeted user to click a malicious link. A successful exploit could allow the attacker to send arbitrary requests that could take unauthorized actions on behalf of the targeted user. **CVE ID : CVE-2020-3456**		
firepower_9300_sm-36					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3457**	N/A	H-CIS-FIRE-031120/1553
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could	N/A	H-CIS-FIRE-031120/1554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3459**		
N/A	21-Oct-20	7.2	A vulnerability in the secure boot process of Cisco FXOS Software could allow an authenticated, local attacker to bypass the secure boot mechanisms. The vulnerability is due to insufficient protections of the secure boot process. An attacker could exploit this vulnerability by injecting code into a specific file that is then referenced during the device boot process. A successful exploit could allow the attacker to break the chain of trust and inject code into the boot process of the device which would be executed at each boot and maintain persistence across reboots. **CVE ID : CVE-2020-3455**	N/A	H-CIS-FIRE-031120/1555
Cross-Site Request Forgery (CSRF)	21-Oct-20	6.8	A vulnerability in the Cisco Firepower Chassis Manager (FCM) of Cisco FXOS Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF)	N/A	H-CIS-FIRE-031120/1556

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attack against a user of an affected device. The vulnerability is due to insufficient CSRF protections for the FCM interface. An attacker could exploit this vulnerability by persuading a targeted user to click a malicious link. A successful exploit could allow the attacker to send arbitrary requests that could take unauthorized actions on behalf of the targeted user. **CVE ID : CVE-2020-3456**		
firepower_9300_sm-40					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3457**	N/A	H-CIS-FIRE-031120/1557
Improper Neutralization of Special Elements	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary	N/A	H-CIS-FIRE-031120/1558

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3459**		
N/A	21-Oct-20	7.2	A vulnerability in the secure boot process of Cisco FXOS Software could allow an authenticated, local attacker to bypass the secure boot mechanisms. The vulnerability is due to insufficient protections of the secure boot process. An attacker could exploit this vulnerability by injecting code into a specific file that is then referenced during the device boot process. A successful exploit could allow the attacker to break the chain of trust and inject code into the boot process of the device which would be executed at each boot and maintain persistence across reboots. **CVE ID : CVE-2020-3455**	N/A	H-CIS-FIRE-031120/1559
Cross-Site	21-Oct-20	6.8	A vulnerability in the Cisco	N/A	H-CIS-FIRE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Request Forgery (CSRF)			Firepower Chassis Manager (FCM) of Cisco FXOS Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of an affected device. The vulnerability is due to insufficient CSRF protections for the FCM interface. An attacker could exploit this vulnerability by persuading a targeted user to click a malicious link. A successful exploit could allow the attacker to send arbitrary requests that could take unauthorized actions on behalf of the targeted user. **CVE ID : CVE-2020-3456**		031120/1560
firepower_9300_sm-44					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root	N/A	H-CIS-FIRE-031120/1561

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges. **CVE ID : CVE-2020-3457**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3459**	N/A	H-CIS-FIRE-031120/1562
N/A	21-Oct-20	7.2	A vulnerability in the secure boot process of Cisco FXOS Software could allow an authenticated, local attacker to bypass the secure boot mechanisms. The vulnerability is due to insufficient protections of the secure boot process. An attacker could exploit this vulnerability by injecting code into a specific file that is then referenced during the device boot process. A successful exploit could allow the attacker to break the chain of trust and inject code into the boot process of the	N/A	H-CIS-FIRE-031120/1563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device which would be executed at each boot and maintain persistence across reboots. **CVE ID : CVE-2020-3455**		
Cross-Site Request Forgery (CSRF)	21-Oct-20	6.8	A vulnerability in the Cisco Firepower Chassis Manager (FCM) of Cisco FXOS Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of an affected device. The vulnerability is due to insufficient CSRF protections for the FCM interface. An attacker could exploit this vulnerability by persuading a targeted user to click a malicious link. A successful exploit could allow the attacker to send arbitrary requests that could take unauthorized actions on behalf of the targeted user. **CVE ID : CVE-2020-3456**	N/A	H-CIS-FIRE-031120/1564
firepower_9300_sm-44_x_3					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and	N/A	H-CIS-FIRE-031120/1565

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3457**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3459**	N/A	H-CIS-FIRE-031120/1566
N/A	21-Oct-20	7.2	A vulnerability in the secure boot process of Cisco FXOS Software could allow an authenticated, local attacker to bypass the secure boot mechanisms. The vulnerability is due to insufficient protections of the secure boot process. An attacker could exploit this vulnerability by injecting code into a specific file that is	N/A	H-CIS-FIRE-031120/1567

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			then referenced during the device boot process. A successful exploit could allow the attacker to break the chain of trust and inject code into the boot process of the device which would be executed at each boot and maintain persistence across reboots. **CVE ID : CVE-2020-3455**		
Cross-Site Request Forgery (CSRF)	21-Oct-20	6.8	A vulnerability in the Cisco Firepower Chassis Manager (FCM) of Cisco FXOS Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of an affected device. The vulnerability is due to insufficient CSRF protections for the FCM interface. An attacker could exploit this vulnerability by persuading a targeted user to click a malicious link. A successful exploit could allow the attacker to send arbitrary requests that could take unauthorized actions on behalf of the targeted user. **CVE ID : CVE-2020-3456**	N/A	H-CIS-FIRE-031120/1568
firepower_9300_sm-48					
Improper Neutralization of Special Elements used in an OS Command	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The	N/A	H-CIS-FIRE-031120/1569

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3457**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3459**	N/A	H-CIS-FIRE-031120/1570
N/A	21-Oct-20	7.2	A vulnerability in the secure boot process of Cisco FXOS Software could allow an authenticated, local attacker to bypass the secure boot mechanisms. The	N/A	H-CIS-FIRE-031120/1571

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to insufficient protections of the secure boot process. An attacker could exploit this vulnerability by injecting code into a specific file that is then referenced during the device boot process. A successful exploit could allow the attacker to break the chain of trust and inject code into the boot process of the device which would be executed at each boot and maintain persistence across reboots. **CVE ID : CVE-2020-3455**		
Cross-Site Request Forgery (CSRF)	21-Oct-20	6.8	A vulnerability in the Cisco Firepower Chassis Manager (FCM) of Cisco FXOS Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of an affected device. The vulnerability is due to insufficient CSRF protections for the FCM interface. An attacker could exploit this vulnerability by persuading a targeted user to click a malicious link. A successful exploit could allow the attacker to send arbitrary requests that could take unauthorized actions on behalf of the targeted user. **CVE ID : CVE-2020-3456**	N/A	H-CIS-FIRE-031120/1572
firepower_9300_sm-56					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3457**	N/A	H-CIS-FIRE-031120/1573
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3459**	N/A	H-CIS-FIRE-031120/1574

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	21-Oct-20	7.2	A vulnerability in the secure boot process of Cisco FXOS Software could allow an authenticated, local attacker to bypass the secure boot mechanisms. The vulnerability is due to insufficient protections of the secure boot process. An attacker could exploit this vulnerability by injecting code into a specific file that is then referenced during the device boot process. A successful exploit could allow the attacker to break the chain of trust and inject code into the boot process of the device which would be executed at each boot and maintain persistence across reboots. **CVE ID : CVE-2020-3455**	N/A	H-CIS-FIRE-031120/1575
Cross-Site Request Forgery (CSRF)	21-Oct-20	6.8	A vulnerability in the Cisco Firepower Chassis Manager (FCM) of Cisco FXOS Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of an affected device. The vulnerability is due to insufficient CSRF protections for the FCM interface. An attacker could exploit this vulnerability by persuading a targeted user to click a malicious link. A successful exploit could allow the attacker to send arbitrary	N/A	H-CIS-FIRE-031120/1576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			requests that could take unauthorized actions on behalf of the targeted user. **CVE ID : CVE-2020-3456**		
firepower_9300_sm-56_x_3					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3457**	N/A	H-CIS-FIRE-031120/1577
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Oct-20	7.2	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow	N/A	H-CIS-FIRE-031120/1578

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the attacker to execute commands on the underlying operating system with root privileges. **CVE ID : CVE-2020-3459**		
N/A	21-Oct-20	7.2	A vulnerability in the secure boot process of Cisco FXOS Software could allow an authenticated, local attacker to bypass the secure boot mechanisms. The vulnerability is due to insufficient protections of the secure boot process. An attacker could exploit this vulnerability by injecting code into a specific file that is then referenced during the device boot process. A successful exploit could allow the attacker to break the chain of trust and inject code into the boot process of the device which would be executed at each boot and maintain persistence across reboots. **CVE ID : CVE-2020-3455**	N/A	H-CIS-FIRE-031120/1579
Cross-Site Request Forgery (CSRF)	21-Oct-20	6.8	A vulnerability in the Cisco Firepower Chassis Manager (FCM) of Cisco FXOS Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of an affected device. The vulnerability is due to insufficient CSRF protections for the FCM interface. An	N/A	H-CIS-FIRE-031120/1580

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
			attacker could exploit this vulnerability by persuading a targeted user to click a malicious link. A successful exploit could allow the attacker to send arbitrary requests that could take unauthorized actions on behalf of the targeted user. **CVE ID : CVE-2020-3456**		
fireeye					
ex_3500					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-Oct-20	4	eMPS prior to eMPS 9.0 FireEye EX 3500 devices allows remote authenticated users to conduct SQL injection attacks via the sort, sort_by, search{URL], or search[attachment] parameter to the email search feature. **CVE ID : CVE-2020-25034**	N/A	H-FIR-EX_3-031120/1581
free					
freebox_v5					
Authentication Bypass by Spoofing	19-Oct-20	4.3	A DNS rebinding vulnerability in the UPnP MediaServer implementation in Freebox Server before 4.2.3. **CVE ID : CVE-2020-24375**	https://dev.freebox.fr/blog/?p=10222	H-FRE-FREE-031120/1582
Huawei					
e6878-370					
N/A	19-Oct-20	2.7	E6878-370 versions 10.0.3.1(H557SP27C233),10.0.3.1(H563SP21C233) and E6878-870 versions 10.0.3.1(H557SP27C233),10.0.3.1(H563SP11C233) have a	N/A	H-HUA-E687-031120/1583

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial of service vulnerability. The system does not properly check some events, an attacker could launch the events continually, successful exploit could cause reboot of the process. **CVE ID : CVE-2020-9111**		
e6878-870					
N/A	19-Oct-20	2.7	E6878-370 versions 10.0.3.1(H557SP27C233),10.0.3.1(H563SP21C233) and E6878-870 versions 10.0.3.1(H557SP27C233),10.0.3.1(H563SP11C233) have a denial of service vulnerability. The system does not properly check some events, an attacker could launch the events continually, successful exploit could cause reboot of the process. **CVE ID : CVE-2020-9111**	N/A	H-HUA-E687-031120/1584
taurus-an00b					
Improper Privilege Management	19-Oct-20	4.6	Taurus-AN00B versions earlier than 10.1.0.156(C00E155R7P2) have a privilege elevation vulnerability. Due to lack of privilege restrictions on some of the business functions of the device. An attacker could exploit this vulnerability to access the protecting information, resulting in the elevation of the privilege. **CVE ID : CVE-2020-9112**	N/A	H-HUA-TAUR-031120/1585
p30					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	19-Oct-20	6.8	HUAWEI Mate 30 versions earlier than 10.1.0.150(C00E136R5P3) and HUAWEI P30 version earlier than 10.1.0.160(C00E160R2P11) 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 common privilege, successful exploit could cause code execution. **CVE ID : CVE-2020-9263**	N/A	H-HUA-P30-031120/1586
mate_20					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-Oct-20	5.4	HUAWEI Mate 20 versions earlier than 10.0.0.188(C00E74R3P8) have a buffer overflow vulnerability in the Bluetooth module. Due to insufficient input validation, an unauthenticated attacker may craft Bluetooth messages after successful paring, causing buffer overflow. Successful exploit may cause code execution. **CVE ID : CVE-2020-9113**	N/A	H-HUA-MATE-031120/1587
Improper Neutralization of Special Elements in Output Used by a Downstream	19-Oct-20	2.1	HUAWEI Mate 20 versions earlier than 10.1.0.163(C00E160R3P8) have a JavaScript injection vulnerability. A module does not verify a specific input. This could allow attackers to	N/A	H-HUA-MATE-031120/1588

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Component ('Injection')			bypass filter mechanism to launch JavaScript injection. This could compromise normal service of the affected module. **CVE ID : CVE-2020-9092**		
mate_30					
Use After Free	19-Oct-20	6.8	HUAWEI Mate 30 versions earlier than 10.1.0.150(C00E136R5P3) and HUAWEI P30 version earlier than 10.1.0.160(C00E160R2P11) 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 common privilege, successful exploit could cause code execution. **CVE ID : CVE-2020-9263**	N/A	H-HUA-MATE-031120/1589
Juniper					
srx380					
N/A	16-Oct-20	4.3	On Juniper Networks Junos OS devices configured as a DHCP forwarder, the Juniper Networks Dynamic Host Configuration Protocol Daemon (jdhcp) process might crash when receiving a malformed DHCP packet. This issue only affects devices configured as DHCP forwarder with forward-only option, that forward specified	https://kb.juniper.net/JSA11056	H-JUN-SRX3-031120/1590

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			DHCP client packets, without creating a new subscriber session. The jdhcpd daemon automatically restarts without intervention, but continuous receipt of the malformed DHCP packet will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. This issue can be triggered only by DHCPv4, it cannot be triggered by DHCPv6. This issue affects Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S16; 12.3X48 versions prior to 12.3X48-D105 on SRX Series; 14.1X53 versions prior to 14.1X53-D60 on EX and QFX Series; 15.1 versions prior to 15.1R7-S7; 15.1X49 versions prior to 15.1X49-D221, 15.1X49-D230 on SRX Series; 15.1X53 versions prior to 15.1X53-D593 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S5. **CVE ID : CVE-2020-1661**		
Missing Encryption of Sensitive Data	16-Oct-20	2.1	On Juniper Networks SRX Series and NFX Series, a local authenticated user with access to the shell may obtain the Web API service private key that is used to provide encrypted communication between the Juniper device and the authenticator services. Exploitation of this vulnerability may allow an attacker to decrypt the	https://kb.juniper.net/JSA11085	H-JUN-SRX3-031120/1591

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			communications between the Juniper device and the authenticator service. This Web API service is used for authentication services such as the Juniper Identity Management Service, used to obtain user identity for Integrated User Firewall feature, or the integrated ClearPass authentication and enforcement feature. This issue affects Juniper Networks Junos OS on Networks SRX Series and NFX Series: 12.3X48 versions prior to 12.3X48-D105; 15.1X49 versions prior to 15.1X49-D190; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3; 18.1 versions prior to 18.1R3-S7; 18.2 versions prior to 18.2R3; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R1-S7, 18.4R2; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S4, 19.2R2. **CVE ID : CVE-2020-1688**		
qfx5130					
N/A	16-Oct-20	4.3	On Juniper Networks Junos OS devices configured as a DHCP forwarder, the Juniper Networks Dynamic Host Configuration Protocol	https://kb.juniper.net/JSA11056	H-JUN-QFX5-031120/1592

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Daemon (jdhcp) process might crash when receiving a malformed DHCP packet. This issue only affects devices configured as DHCP forwarder with forward-only option, that forward specified DHCP client packets, without creating a new subscriber session. The jdhcpd daemon automatically restarts without intervention, but continuous receipt of the malformed DHCP packet will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. This issue can be triggered only by DHCPv4, it cannot be triggered by DHCPv6. This issue affects Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S16; 12.3X48 versions prior to 12.3X48-D105 on SRX Series; 14.1X53 versions prior to 14.1X53-D60 on EX and QFX Series; 15.1 versions prior to 15.1R7-S7; 15.1X49 versions prior to 15.1X49-D221, 15.1X49-D230 on SRX Series; 15.1X53 versions prior to 15.1X53-D593 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S5. **CVE ID : CVE-2020-1661**		
N/A	16-Oct-20	4.3	On Juniper Networks PTX and QFX Series devices with packet sampling configured using tunnel-observation mpls-over-udp, sampling of a	https://kb.juniper.net/JSA11076	H-JUN-QFX5-031120/1593

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malformed packet can cause the Kernel Routing Table (KRT) queue to become stuck. KRT is the module within the Routing Process Daemon (RPD) that synchronized the routing tables with the forwarding tables in the kernel. This table is then synchronized to the Packet Forwarding Engine (PFE) via the KRT queue. Thus, when KRT queue become stuck, it can lead to unexpected packet forwarding issues. An administrator can monitor the following command to check if there is the KRT queue is stuck: user@device > show krt state ... Number of async queue entries: 65007 <--- this value keep on increasing. When this issue occurs, the following message might appear in the /var/log/messages: DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Too many delayed route/nexthop unrefs. Op 2 err 55, rtsm_id 5:-1, msg type 2 DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Memory usage of M_RTNEXTHOP type = (0) Max size possible for M_RTNEXTHOP type = (7297134592) Current delayed unref = (60000), Current unique delayed unref = (18420), Max delayed unref		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on this platform = (40000) Current delayed weight unref = (60000) Max delayed weight unref on this platform= (400000) curproc = rpd This issue affects Juniper Networks Junos OS on PTX/QFX Series: 17.2X75 versions prior to 17.2X75-D105; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.2X75 versions prior to 18.2X75-D420, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R1-S7, 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R2-S2, 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2. This issue does not affect Juniper Networks Junos OS prior to 18.1R1. **CVE ID : CVE-2020-1679**		
Information Exposure Through Discrepancy	16-Oct-20	5	When configuring stateless firewall filters in Juniper Networks EX4600 and QFX 5000 Series devices using Virtual Extensible LAN protocol (VXLAN), the discard action will fail to discard traffic under certain conditions. Given a firewall filter configuration similar to: family ethernet-switching {	https://kb.juniper.net/JSA11082	H-JUN-QFX5-031120/1594

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			filter L2-VLAN { term ALLOW { from { user-vlan-id 100; } then { accept; } } term NON-MATCH { then { discard; } } when there is only one term containing a 'user-vlan-id' match condition, and no other terms in the firewall filter except discard, the discard action for non-matching traffic will only discard traffic with the same VLAN ID specified under 'user-vlan-id'. Other traffic (e.g. VLAN ID 200) will not be discarded. This unexpected behavior can lead to unintended traffic passing through the interface where the firewall filter is applied. This issue only affects systems using VXLANs. This issue affects Juniper Networks Junos OS on QFX5K Series: 18.1 versions prior to 18.1R3-S7, except 18.1R3; 18.2 versions prior to 18.2R2-S7, 18.2R3-S1; 18.3 versions prior to 18.3R1-S5, 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R1-S7, 18.4R2-S1, 18.4R3; 19.1 versions prior to 19.1R1-S5, 19.1R2; 19.2 versions prior to 19.2R1-S5, 19.2R2. **CVE ID : CVE-2020-1685**		
Uncontrolled Resource Consumption	16-Oct-20	3.3	On Juniper Networks EX4300-MP Series, EX4600 Series and QFX5K Series deployed in a Virtual Chassis configuration, receipt of a	https://kb.juniper.net/JSA11086	H-JUN-QFX5-031120/1595

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			stream of specific layer 2 frames can cause high CPU load, which could lead to traffic interruption. This issue does not occur when the device is deployed in Stand Alone configuration. The offending layer 2 frame packets can originate only from within the broadcast domain where the device is connected. This issue affects Juniper Networks Junos OS on EX4300-MP Series, EX4600 Series and QFX5K Series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S3, 20.1R2. **CVE ID : CVE-2020-1689**		
nfx350					
Insufficiently Protected Credentials	16-Oct-20	2.1	The Juniper Device Manager (JDM) container, used by the disaggregated Junos OS architecture on Juniper Networks NFX350 Series	https://kb.juniper.net/JSA11066	H-JUN-NFX3-031120/1596

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			devices, stores password hashes in the world-readable file /etc/passwd. This is not a security best current practice as it can allow an attacker with access to the local filesystem the ability to brute-force decrypt password hashes stored on the system. This issue affects Juniper Networks Junos OS on NFX350: 19.4 versions prior to 19.4R3; 20.1 versions prior to 20.1R1-S4, 20.1R2. **CVE ID : CVE-2020-1669**		
Missing Encryption of Sensitive Data	16-Oct-20	2.1	On Juniper Networks SRX Series and NFX Series, a local authenticated user with access to the shell may obtain the Web API service private key that is used to provide encrypted communication between the Juniper device and the authenticator services. Exploitation of this vulnerability may allow an attacker to decrypt the communications between the Juniper device and the authenticator service. This Web API service is used for authentication services such as the Juniper Identity Management Service, used to obtain user identity for Integrated User Firewall feature, or the integrated ClearPass authentication and enforcement feature. This issue affects Juniper Networks Junos OS on	https://kb.juniper.net/JSA11085	H-JUN-NFX3-031120/1597

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networks SRX Series and NFX Series: 12.3X48 versions prior to 12.3X48-D105; 15.1X49 versions prior to 15.1X49-D190; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3; 18.1 versions prior to 18.1R3-S7; 18.2 versions prior to 18.2R3; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R1-S7, 18.4R2; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S4, 19.2R2. **CVE ID : CVE-2020-1688**		
ptx10001-36mr					
N/A	16-Oct-20	4.3	On Juniper Networks PTX and QFX Series devices with packet sampling configured using tunnel-observation mpls-over-udp, sampling of a malformed packet can cause the Kernel Routing Table (KRT) queue to become stuck. KRT is the module within the Routing Process Daemon (RPD) that synchronized the routing tables with the forwarding tables in the kernel. This table is then synchronized to the Packet Forwarding Engine (PFE) via the KRT queue. Thus, when KRT queue become stuck, it can	https://kb.juniper.net/JSA11076	H-JUN-PTX1-031120/1598

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to unexpected packet forwarding issues. An administrator can monitor the following command to check if there is the KRT queue is stuck: user@device > show krt state ... Number of async queue entries: 65007 <--- this value keep on increasing. When this issue occurs, the following message might appear in the /var/log/messages: DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Too many delayed route/nexthop unrefs. Op 2 err 55, rtsm_id 5:-1, msg type 2 DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Memory usage of M_RTNEXTHOP type = (0) Max size possible for M_RTNEXTHOP type = (7297134592) Current delayed unref = (60000), Current unique delayed unref = (18420), Max delayed unref on this platform = (40000) Current delayed weight unref = (60000) Max delayed weight unref on this platform= (400000) curproc = rpd This issue affects Juniper Networks Junos OS on PTX/QFX Series: 17.2X75 versions prior to 17.2X75-D105; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.2X75 versions prior to 18.2X75-D420, 18.2X75-D53, 18.2X75-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			D65; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R1-S7, 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R2-S2, 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2. This issue does not affect Juniper Networks Junos OS prior to 18.1R1. **CVE ID : CVE-2020-1679**		
ptx100016					
N/A	16-Oct-20	4.3	On Juniper Networks PTX and QFX Series devices with packet sampling configured using tunnel-observation mpls-over-udp, sampling of a malformed packet can cause the Kernel Routing Table (KRT) queue to become stuck. KRT is the module within the Routing Process Daemon (RPD) that synchronized the routing tables with the forwarding tables in the kernel. This table is then synchronized to the Packet Forwarding Engine (PFE) via the KRT queue. Thus, when KRT queue become stuck, it can lead to unexpected packet forwarding issues. An administrator can monitor the following command to	https://kb.juniper.net/JSA11076	H-JUN-PTX1-031120/1599

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check if there is the KRT queue is stuck: user@device > show krt state ... Number of async queue entries: 65007 <--- this value keep on increasing. When this issue occurs, the following message might appear in the /var/log/messages: DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Too many delayed route/nexthop unrefs. Op 2 err 55, rtsm_id 5:-1, msg type 2 DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Memory usage of M_RTNEXTHOP type = (0) Max size possible for M_RTNEXTHOP type = (7297134592) Current delayed unref = (60000), Current unique delayed unref = (18420), Max delayed unref on this platform = (40000) Current delayed weight unref = (60000) Max delayed weight unref on this platform= (400000) curproc = rpd This issue affects Juniper Networks Junos OS on PTX/QFX Series: 17.2X75 versions prior to 17.2X75-D105; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.2X75 versions prior to 18.2X75-D420, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R1-S7, 18.4R2-S5, 18.4R3-S4; 19.1		

CVSS Scoring Scale	0-1	1-2	2-3	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 prior to 19.1R2-S2, 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2. This issue does not affect Juniper Networks Junos OS prior to 18.1R1. **CVE ID : CVE-2020-1679**		
ptx10004					
N/A	16-Oct-20	4.3	On Juniper Networks PTX and QFX Series devices with packet sampling configured using tunnel-observation mpls-over-udp, sampling of a malformed packet can cause the Kernel Routing Table (KRT) queue to become stuck. KRT is the module within the Routing Process Daemon (RPD) that synchronized the routing tables with the forwarding tables in the kernel. This table is then synchronized to the Packet Forwarding Engine (PFE) via the KRT queue. Thus, when KRT queue become stuck, it can lead to unexpected packet forwarding issues. An administrator can monitor the following command to check if there is the KRT queue is stuck: user@device > show krt state ... Number of async queue entries: 65007	https://kb.juniper.net/JSA11076	H-JUN-PTX1-031120/1600

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<--- this value keep on increasing. When this issue occurs, the following message might appear in the /var/log/messages: DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Too many delayed route/nexthop unrefs. Op 2 err 55, rtsm_id 5:-1, msg type 2 DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Memory usage of M_RTNEXTHOP type = (0) Max size possible for M_RTNEXTHOP type = (7297134592) Current delayed unref = (60000), Current unique delayed unref = (18420), Max delayed unref on this platform = (40000) Current delayed weight unref = (60000) Max delayed weight unref on this platform= (400000) curproc = rpd This issue affects Juniper Networks Junos OS on PTX/QFX Series: 17.2X75 versions prior to 17.2X75-D105; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.2X75 versions prior to 18.2X75-D420, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R1-S7, 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R2-S2, 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2. This issue does not affect Juniper Networks Junos OS prior to 18.1R1. **CVE ID : CVE-2020-1679**		
mx2020					
N/A	16-Oct-20	5	On Juniper Networks MX Series and EX9200 Series, in a certain condition the IPv6 Distributed Denial of Service (DDoS) protection might not take affect when it reaches the threshold condition. The DDoS protection allows the device to continue to function while it is under DDoS attack, protecting both the Routing Engine (RE) and the Flexible PIC Concentrator (FPC) during the DDoS attack. When this issue occurs, the RE and/or the FPC can become overwhelmed, which could disrupt network protocol operations and/or interrupt traffic. This issue does not affect IPv4 DDoS protection. This issue affects MX Series and EX9200 Series with Trio-based PFEs (Packet Forwarding Engines). Please refer to https://kb.juniper.net/KB25385 for the list of Trio-based PFEs. This issue affects Juniper Networks Junos OS on MX series and EX9200	https://kb.juniper.net/JSA11062	H-JUN-MX20-031120/1601

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series: 17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R2-S7, 18.2R3, 18.2R3-S3; 18.2X75 versions prior to 18.2X75-D30; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2. **CVE ID : CVE-2020-1665**		
Incorrect Calculation of Buffer Size	16-Oct-20	5	On Juniper Networks MX Series with MS-MIC or MS-MPC card configured with NAT64 configuration, receipt of a malformed IPv6 packet may crash the MS-PIC component on MS-MIC or MS-MPC. This issue occurs when a multiservice card is translating the malformed IPv6 packet to IPv4 packet. An unauthenticated attacker can continuously send crafted IPv6 packets through the device causing repetitive MS-PIC process crashes, resulting in an extended Denial of Service condition. This issue affects Juniper Networks Junos OS on MX Series: 15.1 versions prior to 15.1R7-S7; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S6; 17.4 versions prior to 17.4R2-S11, 17.4R3;	https://kb.juniper.net/JSA11077	H-JUN-MX20-031120/1602

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D430, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2. **CVE ID : CVE-2020-1680**		
mx204					
N/A	16-Oct-20	5	On Juniper Networks MX Series and EX9200 Series, in a certain condition the IPv6 Distributed Denial of Service (DDoS) protection might not take affect when it reaches the threshold condition. The DDoS protection allows the device to continue to function while it is under DDoS attack, protecting both the Routing Engine (RE) and the Flexible PIC Concentrator (FPC) during the DDoS attack. When this issue occurs, the RE and/or the FPC can become overwhelmed, which could disrupt network protocol operations and/or interrupt traffic. This issue does not affect IPv4 DDoS protection. This issue affects MX Series and EX9200 Series with Trio-based PFEs (Packet Forwarding Engines). Please	https://kb.juniper.net/JSA11062	H-JUN-MX20-031120/1603

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			refer to https://kb.juniper.net/KB25385 for the list of Trio-based PFEs. This issue affects Juniper Networks Junos OS on MX series and EX9200 Series: 17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R2-S7, 18.2R3, 18.2R3-S3; 18.2X75 versions prior to 18.2X75-D30; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2. **CVE ID : CVE-2020-1665**		
Incorrect Calculation of Buffer Size	16-Oct-20	5	On Juniper Networks MX Series with MS-MIC or MS-MPC card configured with NAT64 configuration, receipt of a malformed IPv6 packet may crash the MS-PIC component on MS-MIC or MS-MPC. This issue occurs when a multiservice card is translating the malformed IPv6 packet to IPv4 packet. An unauthenticated attacker can continuously send crafted IPv6 packets through the device causing repetitive MS-PIC process crashes, resulting in an extended Denial of Service condition. This issue affects Juniper Networks Junos OS on MX Series: 15.1 versions prior to 15.1R7-S7; 15.1X53 versions prior to	https://kb.juniper.net/JSA11077	H-JUN-MX20-031120/1604

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			15.1X53-D593; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S6; 17.4 versions prior to 17.4R2-S11, 17.4R3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D430, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2. **CVE ID : CVE-2020-1680**		
mx240					
N/A	16-Oct-20	5	On Juniper Networks MX Series and EX9200 Series, in a certain condition the IPv6 Distributed Denial of Service (DDoS) protection might not take affect when it reaches the threshold condition. The DDoS protection allows the device to continue to function while it is under DDoS attack, protecting both the Routing Engine (RE) and the Flexible PIC Concentrator (FPC) during the DDoS attack. When this issue occurs, the RE and/or the FPC can become overwhelmed, which could disrupt network protocol operations and/or	https://kb.juniper.net/JSA11062	H-JUN-MX24-031120/1605

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interrupt traffic. This issue does not affect IPv4 DDoS protection. This issue affects MX Series and EX9200 Series with Trio-based PFEs (Packet Forwarding Engines). Please refer to https://kb.juniper.net/KB25385 for the list of Trio-based PFEs. This issue affects Juniper Networks Junos OS on MX series and EX9200 Series: 17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R2-S7, 18.2R3, 18.2R3-S3; 18.2X75 versions prior to 18.2X75-D30; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2. **CVE ID : CVE-2020-1665**		
Incorrect Calculation of Buffer Size	16-Oct-20	5	On Juniper Networks MX Series with MS-MIC or MS-MPC card configured with NAT64 configuration, receipt of a malformed IPv6 packet may crash the MS-PIC component on MS-MIC or MS-MPC. This issue occurs when a multiservice card is translating the malformed IPv6 packet to IPv4 packet. An unauthenticated attacker can continuously send crafted IPv6 packets through the device causing repetitive MS-PIC process crashes, resulting	https://kb.juniper.net/JSA11077	H-JUN-MX24-031120/1606

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in an extended Denial of Service condition. This issue affects Juniper Networks Junos OS on MX Series: 15.1 versions prior to 15.1R7-S7; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S6; 17.4 versions prior to 17.4R2-S11, 17.4R3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D430, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2. **CVE ID : CVE-2020-1680**		
mx40					
N/A	16-Oct-20	5	On Juniper Networks MX Series and EX9200 Series, in a certain condition the IPv6 Distributed Denial of Service (DDoS) protection might not take affect when it reaches the threshold condition. The DDoS protection allows the device to continue to function while it is under DDoS attack, protecting both the Routing Engine (RE) and the Flexible PIC Concentrator (FPC)	https://kb.juniper.net/JSA11062	H-JUN-MX40-031120/1607

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			during the DDoS attack. When this issue occurs, the RE and/or the FPC can become overwhelmed, which could disrupt network protocol operations and/or interrupt traffic. This issue does not affect IPv4 DDoS protection. This issue affects MX Series and EX9200 Series with Trio-based PFEs (Packet Forwarding Engines). Please refer to https://kb.juniper.net/KB25385 for the list of Trio-based PFEs. This issue affects Juniper Networks Junos OS on MX series and EX9200 Series: 17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R2-S7, 18.2R3, 18.2R3-S3; 18.2X75 versions prior to 18.2X75-D30; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2. **CVE ID : CVE-2020-1665**		
Incorrect Calculation of Buffer Size	16-Oct-20	5	On Juniper Networks MX Series with MS-MIC or MS-MPC card configured with NAT64 configuration, receipt of a malformed IPv6 packet may crash the MS-PIC component on MS-MIC or MS-MPC. This issue occurs when a multiservice card is translating the malformed	https://kb.juniper.net/JSA11077	H-JUN-MX40-031120/1608

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPv6 packet to IPv4 packet. An unauthenticated attacker can continuously send crafted IPv6 packets through the device causing repetitive MS-PIC process crashes, resulting in an extended Denial of Service condition. This issue affects Juniper Networks Junos OS on MX Series: 15.1 versions prior to 15.1R7-S7; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S6; 17.4 versions prior to 17.4R2-S11, 17.4R3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D430, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2. **CVE ID : CVE-2020-1680**		
mx480					
N/A	16-Oct-20	5	On Juniper Networks MX Series and EX9200 Series, in a certain condition the IPv6 Distributed Denial of Service (DDoS) protection might not take affect when it reaches the threshold condition. The	https://kb.juniper.net/JSA11062	H-JUN-MX48-031120/1609

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			DDoS protection allows the device to continue to function while it is under DDoS attack, protecting both the Routing Engine (RE) and the Flexible PIC Concentrator (FPC) during the DDoS attack. When this issue occurs, the RE and/or the FPC can become overwhelmed, which could disrupt network protocol operations and/or interrupt traffic. This issue does not affect IPv4 DDoS protection. This issue affects MX Series and EX9200 Series with Trio-based PFEs (Packet Forwarding Engines). Please refer to https://kb.juniper.net/KB25385 for the list of Trio-based PFEs. This issue affects Juniper Networks Junos OS on MX series and EX9200 Series: 17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R2-S7, 18.2R3, 18.2R3-S3; 18.2X75 versions prior to 18.2X75-D30; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2. **CVE ID : CVE-2020-1665**		
Incorrect Calculation of Buffer Size	16-Oct-20	5	On Juniper Networks MX Series with MS-MIC or MS-MPC card configured with NAT64 configuration, receipt	https://kb.juniper.net/JSA11077	H-JUN-MX48-031120/1610

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of a malformed IPv6 packet may crash the MS-PIC component on MS-MIC or MS-MPC. This issue occurs when a multiservice card is translating the malformed IPv6 packet to IPv4 packet. An unauthenticated attacker can continuously send crafted IPv6 packets through the device causing repetitive MS-PIC process crashes, resulting in an extended Denial of Service condition. This issue affects Juniper Networks Junos OS on MX Series: 15.1 versions prior to 15.1R7-S7; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S6; 17.4 versions prior to 17.4R2-S11, 17.4R3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D430, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2. **CVE ID : CVE-2020-1680**		
mx5					
N/A	16-Oct-20	5	On Juniper Networks MX	https://kb.ju	H-JUN-MX5-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series and EX9200 Series, in a certain condition the IPv6 Distributed Denial of Service (DDoS) protection might not take affect when it reaches the threshold condition. The DDoS protection allows the device to continue to function while it is under DDoS attack, protecting both the Routing Engine (RE) and the Flexible PIC Concentrator (FPC) during the DDoS attack. When this issue occurs, the RE and/or the FPC can become overwhelmed, which could disrupt network protocol operations and/or interrupt traffic. This issue does not affect IPv4 DDoS protection. This issue affects MX Series and EX9200 Series with Trio-based PFEs (Packet Forwarding Engines). Please refer to https://kb.juniper.net/KB25385 for the list of Trio-based PFEs. This issue affects Juniper Networks Junos OS on MX series and EX9200 Series: 17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R2-S7, 18.2R3, 18.2R3-S3; 18.2X75 versions prior to 18.2X75-D30; 18.3 versions prior to 18.3R2-S4,	niper.net/JSA11062	031120/1611

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.3R3-S2. **CVE ID : CVE-2020-1665**		
Incorrect Calculation of Buffer Size	16-Oct-20	5	On Juniper Networks MX Series with MS-MIC or MS-MPC card configured with NAT64 configuration, receipt of a malformed IPv6 packet may crash the MS-PIC component on MS-MIC or MS-MPC. This issue occurs when a multiservice card is translating the malformed IPv6 packet to IPv4 packet. An unauthenticated attacker can continuously send crafted IPv6 packets through the device causing repetitive MS-PIC process crashes, resulting in an extended Denial of Service condition. This issue affects Juniper Networks Junos OS on MX Series: 15.1 versions prior to 15.1R7-S7; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S6; 17.4 versions prior to 17.4R2-S11, 17.4R3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D430, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S5,	https://kb.juniper.net/JSA11077	H-JUN-MX5-031120/1612

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.2R2; 19.3 versions prior to 19.3R2. **CVE ID : CVE-2020-1680**		
mx80					
N/A	16-Oct-20	5	On Juniper Networks MX Series and EX9200 Series, in a certain condition the IPv6 Distributed Denial of Service (DDoS) protection might not take affect when it reaches the threshold condition. The DDoS protection allows the device to continue to function while it is under DDoS attack, protecting both the Routing Engine (RE) and the Flexible PIC Concentrator (FPC) during the DDoS attack. When this issue occurs, the RE and/or the FPC can become overwhelmed, which could disrupt network protocol operations and/or interrupt traffic. This issue does not affect IPv4 DDoS protection. This issue affects MX Series and EX9200 Series with Trio-based PFEs (Packet Forwarding Engines). Please refer to https://kb.juniper.net/KB25385 for the list of Trio-based PFEs. This issue affects Juniper Networks Junos OS on MX series and EX9200 Series: 17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110; 17.3 versions prior to 17.3R3-S8; 17.4	https://kb.juniper.net/JSA11062	H-JUN-MX80-031120/1613

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R2-S7, 18.2R3, 18.2R3-S3; 18.2X75 versions prior to 18.2X75-D30; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2. **CVE ID : CVE-2020-1665**		
Incorrect Calculation of Buffer Size	16-Oct-20	5	On Juniper Networks MX Series with MS-MIC or MS-MPC card configured with NAT64 configuration, receipt of a malformed IPv6 packet may crash the MS-PIC component on MS-MIC or MS-MPC. This issue occurs when a multiservice card is translating the malformed IPv6 packet to IPv4 packet. An unauthenticated attacker can continuously send crafted IPv6 packets through the device causing repetitive MS-PIC process crashes, resulting in an extended Denial of Service condition. This issue affects Juniper Networks Junos OS on MX Series: 15.1 versions prior to 15.1R7-S7; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S6; 17.4 versions prior to 17.4R2-S11, 17.4R3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D430, 18.2X75-	https://kb.juniper.net/JSA11077	H-JUN-MX80-031120/1614

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2. **CVE ID : CVE-2020-1680**		
mx960					
N/A	16-Oct-20	5	On Juniper Networks MX Series and EX9200 Series, in a certain condition the IPv6 Distributed Denial of Service (DDoS) protection might not take affect when it reaches the threshold condition. The DDoS protection allows the device to continue to function while it is under DDoS attack, protecting both the Routing Engine (RE) and the Flexible PIC Concentrator (FPC) during the DDoS attack. When this issue occurs, the RE and/or the FPC can become overwhelmed, which could disrupt network protocol operations and/or interrupt traffic. This issue does not affect IPv4 DDoS protection. This issue affects MX Series and EX9200 Series with Trio-based PFEs (Packet Forwarding Engines). Please refer to https://kb.juniper.net/KB25385 for the list of Trio-based PFEs. This issue affects Juniper Networks Junos OS	https://kb.juniper.net/JSA11062	H-JUN-MX96-031120/1615

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on MX series and EX9200 Series: 17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R2-S7, 18.2R3, 18.2R3-S3; 18.2X75 versions prior to 18.2X75-D30; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2. **CVE ID : CVE-2020-1665**		
Incorrect Calculation of Buffer Size	16-Oct-20	5	On Juniper Networks MX Series with MS-MIC or MS-MPC card configured with NAT64 configuration, receipt of a malformed IPv6 packet may crash the MS-PIC component on MS-MIC or MS-MPC. This issue occurs when a multiservice card is translating the malformed IPv6 packet to IPv4 packet. An unauthenticated attacker can continuously send crafted IPv6 packets through the device causing repetitive MS-PIC process crashes, resulting in an extended Denial of Service condition. This issue affects Juniper Networks Junos OS on MX Series: 15.1 versions prior to 15.1R7-S7; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S6; 17.4 versions	https://kb.juniper.net/JSA11077	H-JUN-MX96-031120/1616

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 17.4R2-S11, 17.4R3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D430, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2. **CVE ID : CVE-2020-1680**		
ptx1000					
N/A	16-Oct-20	4.3	On Juniper Networks PTX and QFX Series devices with packet sampling configured using tunnel-observation mpls-over-udp, sampling of a malformed packet can cause the Kernel Routing Table (KRT) queue to become stuck. KRT is the module within the Routing Process Daemon (RPD) that synchronized the routing tables with the forwarding tables in the kernel. This table is then synchronized to the Packet Forwarding Engine (PFE) via the KRT queue. Thus, when KRT queue become stuck, it can lead to unexpected packet forwarding issues. An administrator can monitor the following command to check if there is the KRT	https://kb.juniper.net/JSA11076	H-JUN-PTX1-031120/1617

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			queue is stuck: user@device > show krt state ... Number of async queue entries: 65007 <--- this value keep on increasing. When this issue occurs, the following message might appear in the /var/log/messages: DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Too many delayed route/nexthop unrefs. Op 2 err 55, rtsm_id 5:-1, msg type 2 DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Memory usage of M_RTNEXTHOP type = (0) Max size possible for M_RTNEXTHOP type = (7297134592) Current delayed unref = (60000), Current unique delayed unref = (18420), Max delayed unref on this platform = (40000) Current delayed weight unref = (60000) Max delayed weight unref on this platform= (400000) curproc = rpd This issue affects Juniper Networks Junos OS on PTX/QFX Series: 17.2X75 versions prior to 17.2X75-D105; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.2X75 versions prior to 18.2X75-D420, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R1-S7, 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R2-S2,		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2. This issue does not affect Juniper Networks Junos OS prior to 18.1R1. **CVE ID : CVE-2020-1679**		
ptx10002					
N/A	16-Oct-20	4.3	On Juniper Networks PTX and QFX Series devices with packet sampling configured using tunnel-observation mpls-over-udp, sampling of a malformed packet can cause the Kernel Routing Table (KRT) queue to become stuck. KRT is the module within the Routing Process Daemon (RPD) that synchronized the routing tables with the forwarding tables in the kernel. This table is then synchronized to the Packet Forwarding Engine (PFE) via the KRT queue. Thus, when KRT queue become stuck, it can lead to unexpected packet forwarding issues. An administrator can monitor the following command to check if there is the KRT queue is stuck: user@device > show krt state ... Number of async queue entries: 65007 <--- this value keep on	https://kb.juniper.net/JSA11076	H-JUN-PTX1-031120/1618

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			increasing. When this issue occurs, the following message might appear in the /var/log/messages: DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Too many delayed route/nexthop unrefs. Op 2 err 55, rtsm_id 5:-1, msg type 2 DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Memory usage of M_RTNEXTHOP type = (0) Max size possible for M_RTNEXTHOP type = (7297134592) Current delayed unref = (60000), Current unique delayed unref = (18420), Max delayed unref on this platform = (40000) Current delayed weight unref = (60000) Max delayed weight unref on this platform= (400000) curproc = rpd This issue affects Juniper Networks Junos OS on PTX/QFX Series: 17.2X75 versions prior to 17.2X75-D105; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.2X75 versions prior to 18.2X75-D420, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R1-S7, 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R2-S2, 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S3, 19.3R3; 19.4		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 19.4R1-S2, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2. This issue does not affect Juniper Networks Junos OS prior to 18.1R1. **CVE ID : CVE-2020-1679**		
ptx10008					
N/A	16-Oct-20	4.3	On Juniper Networks PTX and QFX Series devices with packet sampling configured using tunnel-observation mpls-over-udp, sampling of a malformed packet can cause the Kernel Routing Table (KRT) queue to become stuck. KRT is the module within the Routing Process Daemon (RPD) that synchronized the routing tables with the forwarding tables in the kernel. This table is then synchronized to the Packet Forwarding Engine (PFE) via the KRT queue. Thus, when KRT queue become stuck, it can lead to unexpected packet forwarding issues. An administrator can monitor the following command to check if there is the KRT queue is stuck: user@device > show krt state ... Number of async queue entries: 65007 <--- this value keep on increasing. When this issue occurs, the following message might appear in the /var/log/messages: DATE	https://kb.juniper.net/JSA11076	H-JUN-PTX1-031120/1619

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			DEVICE kernel: %KERN-3: rt_pfe_veto: Too many delayed route/nexthop unrefs. Op 2 err 55, rtsm_id 5:-1, msg type 2 DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Memory usage of M_RTNEXTHOP type = (0) Max size possible for M_RTNEXTHOP type = (7297134592) Current delayed unref = (60000), Current unique delayed unref = (18420), Max delayed unref on this platform = (40000) Current delayed weight unref = (60000) Max delayed weight unref on this platform= (400000) curproc = rpd This issue affects Juniper Networks Junos OS on PTX/QFX Series: 17.2X75 versions prior to 17.2X75-D105; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.2X75 versions prior to 18.2X75-D420, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R1-S7, 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R2-S2, 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2. This issue does not		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affect Juniper Networks Junos OS prior to 18.1R1. **CVE ID : CVE-2020-1679**		
ptx3000					
N/A	16-Oct-20	4.3	On Juniper Networks PTX and QFX Series devices with packet sampling configured using tunnel-observation mpls-over-udp, sampling of a malformed packet can cause the Kernel Routing Table (KRT) queue to become stuck. KRT is the module within the Routing Process Daemon (RPD) that synchronized the routing tables with the forwarding tables in the kernel. This table is then synchronized to the Packet Forwarding Engine (PFE) via the KRT queue. Thus, when KRT queue become stuck, it can lead to unexpected packet forwarding issues. An administrator can monitor the following command to check if there is the KRT queue is stuck: user@device > show krt state ... Number of async queue entries: 65007 <--- this value keep on increasing. When this issue occurs, the following message might appear in the /var/log/messages: DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Too many delayed route/nexthop unrefs. Op 2 err 55, rtsm_id	https://kb.juniper.net/JSA11076	H-JUN-PTX3-031120/1620

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			5:-1, msg type 2 DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Memory usage of M_RTNEXTHOP type = (0) Max size possible for M_RTNEXTHOP type = (7297134592) Current delayed unref = (60000), Current unique delayed unref = (18420), Max delayed unref on this platform = (40000) Current delayed weight unref = (60000) Max delayed weight unref on this platform= (400000) curproc = rpd This issue affects Juniper Networks Junos OS on PTX/QFX Series: 17.2X75 versions prior to 17.2X75-D105; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.2X75 versions prior to 18.2X75-D420, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R1-S7, 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R2-S2, 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2. This issue does not affect Juniper Networks Junos OS prior to 18.1R1. **CVE ID : CVE-2020-1679**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ptx5000					
N/A	16-Oct-20	4.3	On Juniper Networks PTX and QFX Series devices with packet sampling configured using tunnel-observation mpls-over-udp, sampling of a malformed packet can cause the Kernel Routing Table (KRT) queue to become stuck. KRT is the module within the Routing Process Daemon (RPD) that synchronized the routing tables with the forwarding tables in the kernel. This table is then synchronized to the Packet Forwarding Engine (PFE) via the KRT queue. Thus, when KRT queue become stuck, it can lead to unexpected packet forwarding issues. An administrator can monitor the following command to check if there is the KRT queue is stuck: user@device > show krt state ... Number of async queue entries: 65007 <--- this value keep on increasing. When this issue occurs, the following message might appear in the /var/log/messages: DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Too many delayed route/nexthop unrefs. Op 2 err 55, rtsm_id 5:-1, msg type 2 DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Memory usage of M_RTNEXTHOP type = (0)	https://kb.juniper.net/JSA11076	H-JUN-PTX5-031120/1621

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Max size possible for M_RTNEXTHOP type = (7297134592) Current delayed unref = (60000), Current unique delayed unref = (18420), Max delayed unref on this platform = (40000) Current delayed weight unref = (60000) Max delayed weight unref on this platform= (400000) curproc = rpd This issue affects Juniper Networks Junos OS on PTX/QFX Series: 17.2X75 versions prior to 17.2X75-D105; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.2X75 versions prior to 18.2X75-D420, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R1-S7, 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R2-S2, 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2. This issue does not affect Juniper Networks Junos OS prior to 18.1R1. **CVE ID : CVE-2020-1679**		
ex4300-mp					
Uncontrolled Resource Consumption	16-Oct-20	3.3	On Juniper Networks EX4300-MP Series, EX4600 Series and QFX5K Series	https://kb.juniper.net/JSA11086	H-JUN-EX43-031120/1622

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			deployed in a Virtual Chassis configuration, receipt of a stream of specific layer 2 frames can cause high CPU load, which could lead to traffic interruption. This issue does not occur when the device is deployed in Stand Alone configuration. The offending layer 2 frame packets can originate only from within the broadcast domain where the device is connected. This issue affects Juniper Networks Junos OS on EX4300-MP Series, EX4600 Series and QFX5K Series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S3, 20.1R2. **CVE ID : CVE-2020-1689**		
ex9200					
N/A	16-Oct-20	4.3	On Juniper Networks Junos OS devices configured as a DHCP forwarder, the Juniper	https://kb.juniper.net/JSA11056	H-JUN-EX92-031120/1623

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networks Dynamic Host Configuration Protocol Daemon (jdhcp) process might crash when receiving a malformed DHCP packet. This issue only affects devices configured as DHCP forwarder with forward-only option, that forward specified DHCP client packets, without creating a new subscriber session. The jdhcpd daemon automatically restarts without intervention, but continuous receipt of the malformed DHCP packet will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. This issue can be triggered only by DHCPv4, it cannot be triggered by DHCPv6. This issue affects Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S16; 12.3X48 versions prior to 12.3X48-D105 on SRX Series; 14.1X53 versions prior to 14.1X53-D60 on EX and QFX Series; 15.1 versions prior to 15.1R7-S7; 15.1X49 versions prior to 15.1X49-D221, 15.1X49-D230 on SRX Series; 15.1X53 versions prior to 15.1X53-D593 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S5. **CVE ID : CVE-2020-1661**		
N/A	16-Oct-20	5	On Juniper Networks MX Series and EX9200 Series, in a certain condition the IPv6	https://kb.juniper.net/JS	H-JUN-EX92-031120/1624

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Distributed Denial of Service (DDoS) protection might not take affect when it reaches the threshold condition. The DDoS protection allows the device to continue to function while it is under DDoS attack, protecting both the Routing Engine (RE) and the Flexible PIC Concentrator (FPC) during the DDoS attack. When this issue occurs, the RE and/or the FPC can become overwhelmed, which could disrupt network protocol operations and/or interrupt traffic. This issue does not affect IPv4 DDoS protection. This issue affects MX Series and EX9200 Series with Trio-based PFEs (Packet Forwarding Engines). Please refer to https://kb.juniper.net/KB25385 for the list of Trio-based PFEs. This issue affects Juniper Networks Junos OS on MX series and EX9200 Series: 17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R2-S7, 18.2R3, 18.2R3-S3; 18.2X75 versions prior to 18.2X75-D30; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2. **CVE ID : CVE-2020-1665**	A11062	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ex9250					
N/A	16-Oct-20	4.3	On Juniper Networks Junos OS devices configured as a DHCP forwarder, the Juniper Networks Dynamic Host Configuration Protocol Daemon (jdhcp) process might crash when receiving a malformed DHCP packet. This issue only affects devices configured as DHCP forwarder with forward-only option, that forward specified DHCP client packets, without creating a new subscriber session. The jdhcpd daemon automatically restarts without intervention, but continuous receipt of the malformed DHCP packet will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. This issue can be triggered only by DHCPv4, it cannot be triggered by DHCPv6. This issue affects Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S16; 12.3X48 versions prior to 12.3X48-D105 on SRX Series; 14.1X53 versions prior to 14.1X53-D60 on EX and QFX Series; 15.1 versions prior to 15.1R7-S7; 15.1X49 versions prior to 15.1X49-D221, 15.1X49-D230 on SRX Series; 15.1X53 versions prior to 15.1X53-D593 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S5.	https://kb.juniper.net/JSA11056	H-JUN-EX92-031120/1625

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1661		
srx4600					
N/A	16-Oct-20	4.3	On Juniper Networks Junos OS devices configured as a DHCP forwarder, the Juniper Networks Dynamic Host Configuration Protocol Daemon (jdhcp) process might crash when receiving a malformed DHCP packet. This issue only affects devices configured as DHCP forwarder with forward-only option, that forward specified DHCP client packets, without creating a new subscriber session. The jdhcpd daemon automatically restarts without intervention, but continuous receipt of the malformed DHCP packet will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. This issue can be triggered only by DHCPv4, it cannot be triggered by DHCPv6. This issue affects Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S16; 12.3X48 versions prior to 12.3X48-D105 on SRX Series; 14.1X53 versions prior to 14.1X53-D60 on EX and QFX Series; 15.1 versions prior to 15.1R7-S7; 15.1X49 versions prior to 15.1X49-D221, 15.1X49-D230 on SRX Series; 15.1X53 versions prior to 15.1X53-D593 on EX2300/EX3400; 16.1	https://kb.juniper.net/JSA11056	H-JUN-SRX4-031120/1626

CVSS Scoring Scale	0-1	1-2	2-3	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 prior to 16.1R7-S5. **CVE ID : CVE-2020-1661**		
Missing Encryption of Sensitive Data	16-Oct-20	2.1	On Juniper Networks SRX Series and NFX Series, a local authenticated user with access to the shell may obtain the Web API service private key that is used to provide encrypted communication between the Juniper device and the authenticator services. Exploitation of this vulnerability may allow an attacker to decrypt the communications between the Juniper device and the authenticator service. This Web API service is used for authentication services such as the Juniper Identity Management Service, used to obtain user identity for Integrated User Firewall feature, or the integrated ClearPass authentication and enforcement feature. This issue affects Juniper Networks Junos OS on Networks SRX Series and NFX Series: 12.3X48 versions prior to 12.3X48-D105; 15.1X49 versions prior to 15.1X49-D190; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3; 18.1 versions prior to 18.1R3-S7; 18.2 versions prior to 18.2R3; 18.3 versions	https://kb.juniper.net/JSA11085	H-JUN-SRX4-031120/1627

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R1-S7, 18.4R2; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S4, 19.2R2. **CVE ID : CVE-2020-1688**		
nfx150					
Improper Input Validation	16-Oct-20	2.1	An input validation vulnerability exists in Juniper Networks Junos OS, allowing an attacker to crash the srxpfe process, causing a Denial of Service (DoS) through the use of specific maintenance commands. The srxpfe process restarts automatically, but continuous execution of the commands could lead to an extended Denial of Service condition. This issue only affects the SRX1500, SRX4100, SRX4200, NFX150, NFX250, and vSRX-based platforms. No other products or platforms are affected by this vulnerability. This issue affects Juniper Networks Junos OS: 15.1X49 versions prior to 15.1X49-D220 on SRX1500, SRX4100, SRX4200, vSRX; 17.4 versions prior to 17.4R3-S3 on SRX1500, SRX4100, SRX4200, vSRX; 18.1 versions prior to 18.1R3-S11 on SRX1500, SRX4100, SRX4200, vSRX, NFX150; 18.2 versions prior to 18.2R3-S5 on SRX1500, SRX4100, SRX4200, vSRX,	https://kb.juniper.net/JSA11079	H-JUN-NFX1-031120/1628

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NFX150, NFX250; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 19.1 versions prior to 19.1R3-S2 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 19.2 versions prior to 19.2R1-S5, 19.2R3 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250. This issue does not affect Junos OS 19.3 or any subsequent version. **CVE ID : CVE-2020-1682**		
Missing Encryption of Sensitive Data	16-Oct-20	2.1	On Juniper Networks SRX Series and NFX Series, a local authenticated user with access to the shell may obtain the Web API service private key that is used to provide encrypted communication between the Juniper device and the authenticator services. Exploitation of this vulnerability may allow an attacker to decrypt the communications between the Juniper device and the authenticator service. This Web API service is used for authentication services such as the Juniper Identity Management Service, used to obtain user identity for Integrated User Firewall	https://kb.juniper.net/JSA11085	H-JUN-NFX1-031120/1629

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
			feature, or the integrated ClearPass authentication and enforcement feature. This issue affects Juniper Networks Junos OS on Networks SRX Series and NFX Series: 12.3X48 versions prior to 12.3X48-D105; 15.1X49 versions prior to 15.1X49-D190; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3; 18.1 versions prior to 18.1R3-S7; 18.2 versions prior to 18.2R3; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R1-S7, 18.4R2; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S4, 19.2R2. **CVE ID : CVE-2020-1688**		
nfx250					
Improper Input Validation	16-Oct-20	2.1	An input validation vulnerability exists in Juniper Networks Junos OS, allowing an attacker to crash the srxpfe process, causing a Denial of Service (DoS) through the use of specific maintenance commands. The srxpfe process restarts automatically, but continuous execution of the commands could lead to an extended Denial of Service condition. This issue only affects the	https://kb.juniper.net/JSA11079	H-JUN-NFX2-031120/1630

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SRX1500, SRX4100, SRX4200, NFX150, NFX250, and vSRX-based platforms. No other products or platforms are affected by this vulnerability. This issue affects Juniper Networks Junos OS: 15.1X49 versions prior to 15.1X49-D220 on SRX1500, SRX4100, SRX4200, vSRX; 17.4 versions prior to 17.4R3-S3 on SRX1500, SRX4100, SRX4200, vSRX; 18.1 versions prior to 18.1R3-S11 on SRX1500, SRX4100, SRX4200, vSRX, NFX150; 18.2 versions prior to 18.2R3-S5 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 19.1 versions prior to 19.1R3-S2 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 19.2 versions prior to 19.2R1-S5, 19.2R3 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250. This issue does not affect Junos OS 19.3 or any subsequent version. **CVE ID : CVE-2020-1682**		
Missing Encryption of Sensitive	16-Oct-20	2.1	On Juniper Networks SRX Series and NFX Series, a local authenticated user with	https://kb.juniper.net/JS	H-JUN-NFX2-031120/1631

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Data			access to the shell may obtain the Web API service private key that is used to provide encrypted communication between the Juniper device and the authenticator services. Exploitation of this vulnerability may allow an attacker to decrypt the communications between the Juniper device and the authenticator service. This Web API service is used for authentication services such as the Juniper Identity Management Service, used to obtain user identity for Integrated User Firewall feature, or the integrated ClearPass authentication and enforcement feature. This issue affects Juniper Networks Junos OS on Networks SRX Series and NFX Series: 12.3X48 versions prior to 12.3X48-D105; 15.1X49 versions prior to 15.1X49-D190; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3; 18.1 versions prior to 18.1R3-S7; 18.2 versions prior to 18.2R3; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R1-S7, 18.4R2; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S4,	A11085	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.2R2. **CVE ID : CVE-2020-1688**		
ptx10003					
N/A	16-Oct-20	4.3	On Juniper Networks PTX and QFX Series devices with packet sampling configured using tunnel-observation mpls-over-udp, sampling of a malformed packet can cause the Kernel Routing Table (KRT) queue to become stuck. KRT is the module within the Routing Process Daemon (RPD) that synchronized the routing tables with the forwarding tables in the kernel. This table is then synchronized to the Packet Forwarding Engine (PFE) via the KRT queue. Thus, when KRT queue become stuck, it can lead to unexpected packet forwarding issues. An administrator can monitor the following command to check if there is the KRT queue is stuck: user@device > show krt state ... Number of async queue entries: 65007 <--- this value keep on increasing. When this issue occurs, the following message might appear in the /var/log/messages: DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Too many delayed route/nexthop unrefs. Op 2 err 55, rtsm_id 5:-1, msg type 2 DATE	https://kb.juniper.net/JSA11076	H-JUN-PTX1-031120/1632

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			DEVICE kernel: %KERN-3: rt_pfe_veto: Memory usage of M_RTNEXTHOP type = (0) Max size possible for M_RTNEXTHOP type = (7297134592) Current delayed unref = (60000), Current unique delayed unref = (18420), Max delayed unref on this platform = (40000) Current delayed weight unref = (60000) Max delayed weight unref on this platform= (400000) curproc = rpd This issue affects Juniper Networks Junos OS on PTX/QFX Series: 17.2X75 versions prior to 17.2X75-D105; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.2X75 versions prior to 18.2X75-D420, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R1-S7, 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R2-S2, 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2. This issue does not affect Juniper Networks Junos OS prior to 18.1R1. **CVE ID : CVE-2020-1679**		
qfx5220					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Oct-20	4.3	On Juniper Networks Junos OS devices configured as a DHCP forwarder, the Juniper Networks Dynamic Host Configuration Protocol Daemon (jdhcp) process might crash when receiving a malformed DHCP packet. This issue only affects devices configured as DHCP forwarder with forward-only option, that forward specified DHCP client packets, without creating a new subscriber session. The jdhcpd daemon automatically restarts without intervention, but continuous receipt of the malformed DHCP packet will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. This issue can be triggered only by DHCPv4, it cannot be triggered by DHCPv6. This issue affects Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S16; 12.3X48 versions prior to 12.3X48-D105 on SRX Series; 14.1X53 versions prior to 14.1X53-D60 on EX and QFX Series; 15.1 versions prior to 15.1R7-S7; 15.1X49 versions prior to 15.1X49-D221, 15.1X49-D230 on SRX Series; 15.1X53 versions prior to 15.1X53-D593 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S5. **CVE ID : CVE-2020-1661**	https://kb.juniper.net/JSA11056	H-JUN-QFX5-031120/1633

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Oct-20	4.3	On Juniper Networks PTX and QFX Series devices with packet sampling configured using tunnel-observation mpls-over-udp, sampling of a malformed packet can cause the Kernel Routing Table (KRT) queue to become stuck. KRT is the module within the Routing Process Daemon (RPD) that synchronized the routing tables with the forwarding tables in the kernel. This table is then synchronized to the Packet Forwarding Engine (PFE) via the KRT queue. Thus, when KRT queue become stuck, it can lead to unexpected packet forwarding issues. An administrator can monitor the following command to check if there is the KRT queue is stuck: user@device > show krt state ... Number of async queue entries: 65007 <--- this value keep on increasing. When this issue occurs, the following message might appear in the /var/log/messages: DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Too many delayed route/nexthop unrefs. Op 2 err 55, rtsm_id 5:-1, msg type 2 DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Memory usage of M_RTNEXTHOP type = (0) Max size possible for	https://kb.juniper.net/JSA11076	H-JUN-QFX5-031120/1634

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			M_RTNEXTHOP type = (7297134592) Current delayed unref = (60000), Current unique delayed unref = (18420), Max delayed unref on this platform = (40000) Current delayed weight unref = (60000) Max delayed weight unref on this platform= (400000) curproc = rpd This issue affects Juniper Networks Junos OS on PTX/QFX Series: 17.2X75 versions prior to 17.2X75-D105; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.2X75 versions prior to 18.2X75-D420, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R1-S7, 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R2-S2, 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2. This issue does not affect Juniper Networks Junos OS prior to 18.1R1. **CVE ID : CVE-2020-1679**		
Information Exposure Through Discrepancy	16-Oct-20	5	When configuring stateless firewall filters in Juniper Networks EX4600 and QFX 5000 Series devices using Virtual Extensible LAN protocol (VXLAN), the discard	https://kb.juniper.net/JSA11082	H-JUN-QFX5-031120/1635

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			action will fail to discard traffic under certain conditions. Given a firewall filter configuration similar to: family ethernet-switching { filter L2-VLAN { term ALLOW { from { user-vlan-id 100; } then { accept; } } term NON-MATCH { then { discard; } } when there is only one term containing a 'user-vlan-id' match condition, and no other terms in the firewall filter except discard, the discard action for non-matching traffic will only discard traffic with the same VLAN ID specified under 'user-vlan-id'. Other traffic (e.g. VLAN ID 200) will not be discarded. This unexpected behavior can lead to unintended traffic passing through the interface where the firewall filter is applied. This issue only affects systems using VXLANs. This issue affects Juniper Networks Junos OS on QFX5K Series: 18.1 versions prior to 18.1R3-S7, except 18.1R3; 18.2 versions prior to 18.2R2-S7, 18.2R3-S1; 18.3 versions prior to 18.3R1-S5, 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R1-S7, 18.4R2-S1, 18.4R3; 19.1 versions prior to 19.1R1-S5, 19.1R2; 19.2 versions prior to 19.2R1-S5, 19.2R2. **CVE ID : CVE-2020-1685**		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mx10000					
N/A	16-Oct-20	5	On Juniper Networks MX Series and EX9200 Series, in a certain condition the IPv6 Distributed Denial of Service (DDoS) protection might not take affect when it reaches the threshold condition. The DDoS protection allows the device to continue to function while it is under DDoS attack, protecting both the Routing Engine (RE) and the Flexible PIC Concentrator (FPC) during the DDoS attack. When this issue occurs, the RE and/or the FPC can become overwhelmed, which could disrupt network protocol operations and/or interrupt traffic. This issue does not affect IPv4 DDoS protection. This issue affects MX Series and EX9200 Series with Trio-based PFEs (Packet Forwarding Engines). Please refer to https://kb.juniper.net/KB25385 for the list of Trio-based PFEs. This issue affects Juniper Networks Junos OS on MX series and EX9200 Series: 17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R2-S7, 18.2R3, 18.2R3-S3; 18.2X75 versions	https://kb.juniper.net/JSA11062	H-JUN-MX10-031120/1636

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 18.2X75-D30; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2. **CVE ID : CVE-2020-1665**		
Incorrect Calculation of Buffer Size	16-Oct-20	5	On Juniper Networks MX Series with MS-MIC or MS-MPC card configured with NAT64 configuration, receipt of a malformed IPv6 packet may crash the MS-PIC component on MS-MIC or MS-MPC. This issue occurs when a multiservice card is translating the malformed IPv6 packet to IPv4 packet. An unauthenticated attacker can continuously send crafted IPv6 packets through the device causing repetitive MS-PIC process crashes, resulting in an extended Denial of Service condition. This issue affects Juniper Networks Junos OS on MX Series: 15.1 versions prior to 15.1R7-S7; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S6; 17.4 versions prior to 17.4R2-S11, 17.4R3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D430, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R2-S5, 18.4R3; 19.1	https://kb.juniper.net/JSA11077	H-JUN-MX10-031120/1637

CVSS Scoring Scale	0-1	1-2	2-3	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 prior to 19.1R2; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2. **CVE ID : CVE-2020-1680**		
srx1500					
N/A	16-Oct-20	4.3	On Juniper Networks Junos OS devices configured as a DHCP forwarder, the Juniper Networks Dynamic Host Configuration Protocol Daemon (jdhcp) process might crash when receiving a malformed DHCP packet. This issue only affects devices configured as DHCP forwarder with forward-only option, that forward specified DHCP client packets, without creating a new subscriber session. The jdhcpd daemon automatically restarts without intervention, but continuous receipt of the malformed DHCP packet will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. This issue can be triggered only by DHCPv4, it cannot be triggered by DHCPv6. This issue affects Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S16; 12.3X48 versions prior to 12.3X48-D105 on SRX Series; 14.1X53 versions prior to 14.1X53-D60 on EX and QFX Series; 15.1 versions prior to 15.1R7-S7; 15.1X49	https://kb.juniper.net/JSA11056	H-JUN-SRX1-031120/1638

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 15.1X49-D221, 15.1X49-D230 on SRX Series; 15.1X53 versions prior to 15.1X53-D593 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S5. **CVE ID : CVE-2020-1661**		
Improper Input Validation	16-Oct-20	2.1	An input validation vulnerability exists in Juniper Networks Junos OS, allowing an attacker to crash the srxpfe process, causing a Denial of Service (DoS) through the use of specific maintenance commands. The srxpfe process restarts automatically, but continuous execution of the commands could lead to an extended Denial of Service condition. This issue only affects the SRX1500, SRX4100, SRX4200, NFX150, NFX250, and vSRX-based platforms. No other products or platforms are affected by this vulnerability. This issue affects Juniper Networks Junos OS: 15.1X49 versions prior to 15.1X49-D220 on SRX1500, SRX4100, SRX4200, vSRX; 17.4 versions prior to 17.4R3-S3 on SRX1500, SRX4100, SRX4200, vSRX; 18.1 versions prior to 18.1R3-S11 on SRX1500, SRX4100, SRX4200, vSRX, NFX150; 18.2 versions prior to 18.2R3-S5 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 18.3 versions prior to 18.3R2-S4,	https://kb.juniper.net/JSA11079	H-JUN-SRX1-031120/1639

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.3R3-S3 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 19.1 versions prior to 19.1R3-S2 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 19.2 versions prior to 19.2R1-S5, 19.2R3 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250. This issue does not affect Junos OS 19.3 or any subsequent version. **CVE ID : CVE-2020-1682**		
Missing Encryption of Sensitive Data	16-Oct-20	2.1	On Juniper Networks SRX Series and NFX Series, a local authenticated user with access to the shell may obtain the Web API service private key that is used to provide encrypted communication between the Juniper device and the authenticator services. Exploitation of this vulnerability may allow an attacker to decrypt the communications between the Juniper device and the authenticator service. This Web API service is used for authentication services such as the Juniper Identity Management Service, used to obtain user identity for Integrated User Firewall feature, or the integrated ClearPass authentication and	https://kb.juniper.net/JSA11085	H-JUN-SRX1-031120/1640

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			enforcement feature. This issue affects Juniper Networks Junos OS on Networks SRX Series and NFX Series: 12.3X48 versions prior to 12.3X48-D105; 15.1X49 versions prior to 15.1X49-D190; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3; 18.1 versions prior to 18.1R3-S7; 18.2 versions prior to 18.2R3; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R1-S7, 18.4R2; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S4, 19.2R2. **CVE ID : CVE-2020-1688**		
srx300					
N/A	16-Oct-20	4.3	On Juniper Networks Junos OS devices configured as a DHCP forwarder, the Juniper Networks Dynamic Host Configuration Protocol Daemon (jdhcp) process might crash when receiving a malformed DHCP packet. This issue only affects devices configured as DHCP forwarder with forward-only option, that forward specified DHCP client packets, without creating a new subscriber session. The jdhcpd daemon automatically restarts	https://kb.juniper.net/JSA11056	H-JUN-SRX3-031120/1641

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			without intervention, but continuous receipt of the malformed DHCP packet will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. This issue can be triggered only by DHCPv4, it cannot be triggered by DHCPv6. This issue affects Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S16; 12.3X48 versions prior to 12.3X48-D105 on SRX Series; 14.1X53 versions prior to 14.1X53-D60 on EX and QFX Series; 15.1 versions prior to 15.1R7-S7; 15.1X49 versions prior to 15.1X49-D221, 15.1X49-D230 on SRX Series; 15.1X53 versions prior to 15.1X53-D593 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S5. **CVE ID : CVE-2020-1661**		
Missing Encryption of Sensitive Data	16-Oct-20	2.1	On Juniper Networks SRX Series and NFX Series, a local authenticated user with access to the shell may obtain the Web API service private key that is used to provide encrypted communication between the Juniper device and the authenticator services. Exploitation of this vulnerability may allow an attacker to decrypt the communications between the Juniper device and the authenticator service. This Web API service is used for	https://kb.juniper.net/JSA11085	H-JUN-SRX3-031120/1642

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
			authentication services such as the Juniper Identity Management Service, used to obtain user identity for Integrated User Firewall feature, or the integrated ClearPass authentication and enforcement feature. This issue affects Juniper Networks Junos OS on Networks SRX Series and NFX Series: 12.3X48 versions prior to 12.3X48-D105; 15.1X49 versions prior to 15.1X49-D190; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3; 18.1 versions prior to 18.1R3-S7; 18.2 versions prior to 18.2R3; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R1-S7, 18.4R2; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S4, 19.2R2. **CVE ID : CVE-2020-1688**		
srx320					
N/A	16-Oct-20	4.3	On Juniper Networks Junos OS devices configured as a DHCP forwarder, the Juniper Networks Dynamic Host Configuration Protocol Daemon (jdhcp) process might crash when receiving a malformed DHCP packet. This issue only affects devices	https://kb.juniper.net/JSA11056	H-JUN-SRX3-031120/1643

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			configured as DHCP forwarder with forward-only option, that forward specified DHCP client packets, without creating a new subscriber session. The jdhcpd daemon automatically restarts without intervention, but continuous receipt of the malformed DHCP packet will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. This issue can be triggered only by DHCPv4, it cannot be triggered by DHCPv6. This issue affects Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S16; 12.3X48 versions prior to 12.3X48-D105 on SRX Series; 14.1X53 versions prior to 14.1X53-D60 on EX and QFX Series; 15.1 versions prior to 15.1R7-S7; 15.1X49 versions prior to 15.1X49-D221, 15.1X49-D230 on SRX Series; 15.1X53 versions prior to 15.1X53-D593 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S5. **CVE ID : CVE-2020-1661**		
Missing Encryption of Sensitive Data	16-Oct-20	2.1	On Juniper Networks SRX Series and NFX Series, a local authenticated user with access to the shell may obtain the Web API service private key that is used to provide encrypted communication between the Juniper device and the authenticator	https://kb.juniper.net/JSA11085	H-JUN-SRX3-031120/1644

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			services. Exploitation of this vulnerability may allow an attacker to decrypt the communications between the Juniper device and the authenticator service. This Web API service is used for authentication services such as the Juniper Identity Management Service, used to obtain user identity for Integrated User Firewall feature, or the integrated ClearPass authentication and enforcement feature. This issue affects Juniper Networks Junos OS on Networks SRX Series and NFX Series: 12.3X48 versions prior to 12.3X48-D105; 15.1X49 versions prior to 15.1X49-D190; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3; 18.1 versions prior to 18.1R3-S7; 18.2 versions prior to 18.2R3; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R1-S7, 18.4R2; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S4, 19.2R2. **CVE ID : CVE-2020-1688**		
srx340					
N/A	16-Oct-20	4.3	On Juniper Networks Junos OS devices configured as a	https://kb.juniper.net/JS	H-JUN-SRX3-031120/1645

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			DHCP forwarder, the Juniper Networks Dynamic Host Configuration Protocol Daemon (jdhcp) process might crash when receiving a malformed DHCP packet. This issue only affects devices configured as DHCP forwarder with forward-only option, that forward specified DHCP client packets, without creating a new subscriber session. The jdhcpd daemon automatically restarts without intervention, but continuous receipt of the malformed DHCP packet will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. This issue can be triggered only by DHCPv4, it cannot be triggered by DHCPv6. This issue affects Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S16; 12.3X48 versions prior to 12.3X48-D105 on SRX Series; 14.1X53 versions prior to 14.1X53-D60 on EX and QFX Series; 15.1 versions prior to 15.1R7-S7; 15.1X49 versions prior to 15.1X49-D221, 15.1X49-D230 on SRX Series; 15.1X53 versions prior to 15.1X53-D593 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S5. **CVE ID : CVE-2020-1661**	A11056	
Missing Encryption	16-Oct-20	2.1	On Juniper Networks SRX Series and NFX Series, a local	https://kb.juniper.net/JS	H-JUN-SRX3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Sensitive Data			authenticated user with access to the shell may obtain the Web API service private key that is used to provide encrypted communication between the Juniper device and the authenticator services. Exploitation of this vulnerability may allow an attacker to decrypt the communications between the Juniper device and the authenticator service. This Web API service is used for authentication services such as the Juniper Identity Management Service, used to obtain user identity for Integrated User Firewall feature, or the integrated ClearPass authentication and enforcement feature. This issue affects Juniper Networks Junos OS on Networks SRX Series and NFX Series: 12.3X48 versions prior to 12.3X48-D105; 15.1X49 versions prior to 15.1X49-D190; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3; 18.1 versions prior to 18.1R3-S7; 18.2 versions prior to 18.2R3; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R1-S7, 18.4R2; 19.1 versions prior to 19.1R2; 19.2	A11085	031120/1646

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
			versions prior to 19.2R1-S4, 19.2R2. **CVE ID : CVE-2020-1688**		
srx345					
N/A	16-Oct-20	4.3	On Juniper Networks Junos OS devices configured as a DHCP forwarder, the Juniper Networks Dynamic Host Configuration Protocol Daemon (jdhcp) process might crash when receiving a malformed DHCP packet. This issue only affects devices configured as DHCP forwarder with forward-only option, that forward specified DHCP client packets, without creating a new subscriber session. The jdhcpd daemon automatically restarts without intervention, but continuous receipt of the malformed DHCP packet will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. This issue can be triggered only by DHCPv4, it cannot be triggered by DHCPv6. This issue affects Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S16; 12.3X48 versions prior to 12.3X48-D105 on SRX Series; 14.1X53 versions prior to 14.1X53-D60 on EX and QFX Series; 15.1 versions prior to 15.1R7-S7; 15.1X49 versions prior to 15.1X49-D221, 15.1X49-D230 on SRX	https://kb.juniper.net/JSA11056	H-JUN-SRX3-031120/1647

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series; 15.1X53 versions prior to 15.1X53-D593 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S5. **CVE ID : CVE-2020-1661**		
Missing Encryption of Sensitive Data	16-Oct-20	2.1	On Juniper Networks SRX Series and NFX Series, a local authenticated user with access to the shell may obtain the Web API service private key that is used to provide encrypted communication between the Juniper device and the authenticator services. Exploitation of this vulnerability may allow an attacker to decrypt the communications between the Juniper device and the authenticator service. This Web API service is used for authentication services such as the Juniper Identity Management Service, used to obtain user identity for Integrated User Firewall feature, or the integrated ClearPass authentication and enforcement feature. This issue affects Juniper Networks Junos OS on Networks SRX Series and NFX Series: 12.3X48 versions prior to 12.3X48-D105; 15.1X49 versions prior to 15.1X49-D190; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3;	https://kb.juniper.net/JSA11085	H-JUN-SRX3-031120/1648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.1 versions prior to 18.1R3-S7; 18.2 versions prior to 18.2R3; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R1-S7, 18.4R2; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S4, 19.2R2. **CVE ID : CVE-2020-1688**		
srx4100					
N/A	16-Oct-20	4.3	On Juniper Networks Junos OS devices configured as a DHCP forwarder, the Juniper Networks Dynamic Host Configuration Protocol Daemon (jdhcp) process might crash when receiving a malformed DHCP packet. This issue only affects devices configured as DHCP forwarder with forward-only option, that forward specified DHCP client packets, without creating a new subscriber session. The jdhcpd daemon automatically restarts without intervention, but continuous receipt of the malformed DHCP packet will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. This issue can be triggered only by DHCPv4, it cannot be triggered by DHCPv6. This issue affects Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S16; 12.3X48 versions prior	https://kb.juniper.net/JSA11056	H-JUN-SRX4-031120/1649

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to 12.3X48-D105 on SRX Series; 14.1X53 versions prior to 14.1X53-D60 on EX and QFX Series; 15.1 versions prior to 15.1R7-S7; 15.1X49 versions prior to 15.1X49-D221, 15.1X49-D230 on SRX Series; 15.1X53 versions prior to 15.1X53-D593 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S5. **CVE ID : CVE-2020-1661**		
Improper Input Validation	16-Oct-20	2.1	An input validation vulnerability exists in Juniper Networks Junos OS, allowing an attacker to crash the srxpfe process, causing a Denial of Service (DoS) through the use of specific maintenance commands. The srxpfe process restarts automatically, but continuous execution of the commands could lead to an extended Denial of Service condition. This issue only affects the SRX1500, SRX4100, SRX4200, NFX150, NFX250, and vSRX-based platforms. No other products or platforms are affected by this vulnerability. This issue affects Juniper Networks Junos OS: 15.1X49 versions prior to 15.1X49-D220 on SRX1500, SRX4100, SRX4200, vSRX; 17.4 versions prior to 17.4R3-S3 on SRX1500, SRX4100, SRX4200, vSRX; 18.1 versions prior to 18.1R3-S11 on SRX1500, SRX4100, SRX4200, vSRX,	https://kb.juniper.net/JSA11079	H-JUN-SRX4-031120/1650

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NFX150; 18.2 versions prior to 18.2R3-S5 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 19.1 versions prior to 19.1R3-S2 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 19.2 versions prior to 19.2R1-S5, 19.2R3 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250. This issue does not affect Junos OS 19.3 or any subsequent version. **CVE ID : CVE-2020-1682**		
Missing Encryption of Sensitive Data	16-Oct-20	2.1	On Juniper Networks SRX Series and NFX Series, a local authenticated user with access to the shell may obtain the Web API service private key that is used to provide encrypted communication between the Juniper device and the authenticator services. Exploitation of this vulnerability may allow an attacker to decrypt the communications between the Juniper device and the authenticator service. This Web API service is used for authentication services such as the Juniper Identity	https://kb.juniper.net/JSA11085	H-JUN-SRX4-031120/1651

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Management Service, used to obtain user identity for Integrated User Firewall feature, or the integrated ClearPass authentication and enforcement feature. This issue affects Juniper Networks Junos OS on Networks SRX Series and NFX Series: 12.3X48 versions prior to 12.3X48-D105; 15.1X49 versions prior to 15.1X49-D190; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3; 18.1 versions prior to 18.1R3-S7; 18.2 versions prior to 18.2R3; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R1-S7, 18.4R2; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S4, 19.2R2. **CVE ID : CVE-2020-1688**		
srx4200					
N/A	16-Oct-20	4.3	On Juniper Networks Junos OS devices configured as a DHCP forwarder, the Juniper Networks Dynamic Host Configuration Protocol Daemon (jdhcp) process might crash when receiving a malformed DHCP packet. This issue only affects devices configured as DHCP forwarder with forward-only	https://kb.juniper.net/JSA11056	H-JUN-SRX4-031120/1652

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			option, that forward specified DHCP client packets, without creating a new subscriber session. The jdhcpd daemon automatically restarts without intervention, but continuous receipt of the malformed DHCP packet will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. This issue can be triggered only by DHCPv4, it cannot be triggered by DHCPv6. This issue affects Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S16; 12.3X48 versions prior to 12.3X48-D105 on SRX Series; 14.1X53 versions prior to 14.1X53-D60 on EX and QFX Series; 15.1 versions prior to 15.1R7-S7; 15.1X49 versions prior to 15.1X49-D221, 15.1X49-D230 on SRX Series; 15.1X53 versions prior to 15.1X53-D593 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S5. **CVE ID : CVE-2020-1661**		
Improper Input Validation	16-Oct-20	2.1	An input validation vulnerability exists in Juniper Networks Junos OS, allowing an attacker to crash the srxpfe process, causing a Denial of Service (DoS) through the use of specific maintenance commands. The srxpfe process restarts automatically, but continuous execution of the commands	https://kb.juniper.net/JSA11079	H-JUN-SRX4-031120/1653

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could lead to an extended Denial of Service condition. This issue only affects the SRX1500, SRX4100, SRX4200, NFX150, NFX250, and vSRX-based platforms. No other products or platforms are affected by this vulnerability. This issue affects Juniper Networks Junos OS: 15.1X49 versions prior to 15.1X49-D220 on SRX1500, SRX4100, SRX4200, vSRX; 17.4 versions prior to 17.4R3-S3 on SRX1500, SRX4100, SRX4200, vSRX; 18.1 versions prior to 18.1R3-S11 on SRX1500, SRX4100, SRX4200, vSRX, NFX150; 18.2 versions prior to 18.2R3-S5 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 19.1 versions prior to 19.1R3-S2 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250; 19.2 versions prior to 19.2R1-S5, 19.2R3 on SRX1500, SRX4100, SRX4200, vSRX, NFX150, NFX250. This issue does not affect Junos OS 19.3 or any subsequent version. **CVE ID : CVE-2020-1682**		

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
Missing Encryption of Sensitive Data	16-Oct-20	2.1	On Juniper Networks SRX Series and NFX Series, a local authenticated user with access to the shell may obtain the Web API service private key that is used to provide encrypted communication between the Juniper device and the authenticator services. Exploitation of this vulnerability may allow an attacker to decrypt the communications between the Juniper device and the authenticator service. This Web API service is used for authentication services such as the Juniper Identity Management Service, used to obtain user identity for Integrated User Firewall feature, or the integrated ClearPass authentication and enforcement feature. This issue affects Juniper Networks Junos OS on Networks SRX Series and NFX Series: 12.3X48 versions prior to 12.3X48-D105; 15.1X49 versions prior to 15.1X49-D190; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3; 18.1 versions prior to 18.1R3-S7; 18.2 versions prior to 18.2R3; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to	https://kb.juniper.net/JSA11085	H-JUN-SRX4-031120/1654

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.4R1-S7, 18.4R2; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S4, 19.2R2. **CVE ID : CVE-2020-1688**		
srx5400					
N/A	16-Oct-20	4.3	On Juniper Networks Junos OS devices configured as a DHCP forwarder, the Juniper Networks Dynamic Host Configuration Protocol Daemon (jdhcp) process might crash when receiving a malformed DHCP packet. This issue only affects devices configured as DHCP forwarder with forward-only option, that forward specified DHCP client packets, without creating a new subscriber session. The jdhcpd daemon automatically restarts without intervention, but continuous receipt of the malformed DHCP packet will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. This issue can be triggered only by DHCPv4, it cannot be triggered by DHCPv6. This issue affects Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S16; 12.3X48 versions prior to 12.3X48-D105 on SRX Series; 14.1X53 versions prior to 14.1X53-D60 on EX and QFX Series; 15.1 versions prior to 15.1R7-S7; 15.1X49	https://kb.juniper.net/JSA11056	H-JUN-SRX5-031120/1655

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 15.1X49-D221, 15.1X49-D230 on SRX Series; 15.1X53 versions prior to 15.1X53-D593 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S5. **CVE ID : CVE-2020-1661**		
Missing Encryption of Sensitive Data	16-Oct-20	2.1	On Juniper Networks SRX Series and NFX Series, a local authenticated user with access to the shell may obtain the Web API service private key that is used to provide encrypted communication between the Juniper device and the authenticator services. Exploitation of this vulnerability may allow an attacker to decrypt the communications between the Juniper device and the authenticator service. This Web API service is used for authentication services such as the Juniper Identity Management Service, used to obtain user identity for Integrated User Firewall feature, or the integrated ClearPass authentication and enforcement feature. This issue affects Juniper Networks Junos OS on Networks SRX Series and NFX Series: 12.3X48 versions prior to 12.3X48-D105; 15.1X49 versions prior to 15.1X49-D190; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to	https://kb.juniper.net/JSA11085	H-JUN-SRX5-031120/1656

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3; 18.1 versions prior to 18.1R3-S7; 18.2 versions prior to 18.2R3; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R1-S7, 18.4R2; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S4, 19.2R2. **CVE ID : CVE-2020-1688**		
srx550					
N/A	16-Oct-20	4.3	On Juniper Networks Junos OS devices configured as a DHCP forwarder, the Juniper Networks Dynamic Host Configuration Protocol Daemon (jdhcp) process might crash when receiving a malformed DHCP packet. This issue only affects devices configured as DHCP forwarder with forward-only option, that forward specified DHCP client packets, without creating a new subscriber session. The jdhcpd daemon automatically restarts without intervention, but continuous receipt of the malformed DHCP packet will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. This issue can be triggered only by DHCPv4, it cannot be triggered by DHCPv6. This issue affects Juniper Networks Junos OS: 12.3	https://kb.juniper.net/JSA11056	H-JUN-SRX5-031120/1657

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 12.3R12-S16; 12.3X48 versions prior to 12.3X48-D105 on SRX Series; 14.1X53 versions prior to 14.1X53-D60 on EX and QFX Series; 15.1 versions prior to 15.1R7-S7; 15.1X49 versions prior to 15.1X49-D221, 15.1X49-D230 on SRX Series; 15.1X53 versions prior to 15.1X53-D593 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S5. **CVE ID : CVE-2020-1661**		
Missing Encryption of Sensitive Data	16-Oct-20	2.1	On Juniper Networks SRX Series and NFX Series, a local authenticated user with access to the shell may obtain the Web API service private key that is used to provide encrypted communication between the Juniper device and the authenticator services. Exploitation of this vulnerability may allow an attacker to decrypt the communications between the Juniper device and the authenticator service. This Web API service is used for authentication services such as the Juniper Identity Management Service, used to obtain user identity for Integrated User Firewall feature, or the integrated ClearPass authentication and enforcement feature. This issue affects Juniper Networks Junos OS on Networks SRX Series and NFX	https://kb.juniper.net/JSA11085	H-JUN-SRX5-031120/1658

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series: 12.3X48 versions prior to 12.3X48-D105; 15.1X49 versions prior to 15.1X49-D190; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3; 18.1 versions prior to 18.1R3-S7; 18.2 versions prior to 18.2R3; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R1-S7, 18.4R2; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S4, 19.2R2. **CVE ID : CVE-2020-1688**		
srx5600					
N/A	16-Oct-20	4.3	On Juniper Networks Junos OS devices configured as a DHCP forwarder, the Juniper Networks Dynamic Host Configuration Protocol Daemon (jdhcp) process might crash when receiving a malformed DHCP packet. This issue only affects devices configured as DHCP forwarder with forward-only option, that forward specified DHCP client packets, without creating a new subscriber session. The jdhcpd daemon automatically restarts without intervention, but continuous receipt of the malformed DHCP packet will repeatedly crash jdhcpd,	https://kb.juniper.net/JSA11056	H-JUN-SRX5-031120/1659

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leading to an extended Denial of Service (DoS) condition. This issue can be triggered only by DHCPv4, it cannot be triggered by DHCPv6. This issue affects Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S16; 12.3X48 versions prior to 12.3X48-D105 on SRX Series; 14.1X53 versions prior to 14.1X53-D60 on EX and QFX Series; 15.1 versions prior to 15.1R7-S7; 15.1X49 versions prior to 15.1X49-D221, 15.1X49-D230 on SRX Series; 15.1X53 versions prior to 15.1X53-D593 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S5. **CVE ID : CVE-2020-1661**		
Missing Encryption of Sensitive Data	16-Oct-20	2.1	On Juniper Networks SRX Series and NFX Series, a local authenticated user with access to the shell may obtain the Web API service private key that is used to provide encrypted communication between the Juniper device and the authenticator services. Exploitation of this vulnerability may allow an attacker to decrypt the communications between the Juniper device and the authenticator service. This Web API service is used for authentication services such as the Juniper Identity Management Service, used to obtain user identity for	https://kb.juniper.net/JSA11085	H-JUN-SRX5-031120/1660

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Integrated User Firewall feature, or the integrated ClearPass authentication and enforcement feature. This issue affects Juniper Networks Junos OS on Networks SRX Series and NFX Series: 12.3X48 versions prior to 12.3X48-D105; 15.1X49 versions prior to 15.1X49-D190; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3; 18.1 versions prior to 18.1R3-S7; 18.2 versions prior to 18.2R3; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R1-S7, 18.4R2; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S4, 19.2R2. **CVE ID : CVE-2020-1688**		
srx5800					
N/A	16-Oct-20	4.3	On Juniper Networks Junos OS devices configured as a DHCP forwarder, the Juniper Networks Dynamic Host Configuration Protocol Daemon (jdhcp) process might crash when receiving a malformed DHCP packet. This issue only affects devices configured as DHCP forwarder with forward-only option, that forward specified DHCP client packets, without	https://kb.juniper.net/JSA11056	H-JUN-SRX5-031120/1661

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			creating a new subscriber session. The jdhcpd daemon automatically restarts without intervention, but continuous receipt of the malformed DHCP packet will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. This issue can be triggered only by DHCPv4, it cannot be triggered by DHCPv6. This issue affects Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S16; 12.3X48 versions prior to 12.3X48-D105 on SRX Series; 14.1X53 versions prior to 14.1X53-D60 on EX and QFX Series; 15.1 versions prior to 15.1R7-S7; 15.1X49 versions prior to 15.1X49-D221, 15.1X49-D230 on SRX Series; 15.1X53 versions prior to 15.1X53-D593 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S5. **CVE ID : CVE-2020-1661**		
Missing Encryption of Sensitive Data	16-Oct-20	2.1	On Juniper Networks SRX Series and NFX Series, a local authenticated user with access to the shell may obtain the Web API service private key that is used to provide encrypted communication between the Juniper device and the authenticator services. Exploitation of this vulnerability may allow an attacker to decrypt the communications between the	https://kb.juniper.net/JSA11085	H-JUN-SRX5-031120/1662

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Juniper device and the authenticator service. This Web API service is used for authentication services such as the Juniper Identity Management Service, used to obtain user identity for Integrated User Firewall feature, or the integrated ClearPass authentication and enforcement feature. This issue affects Juniper Networks Junos OS on Networks SRX Series and NFX Series: 12.3X48 versions prior to 12.3X48-D105; 15.1X49 versions prior to 15.1X49-D190; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3; 18.1 versions prior to 18.1R3-S7; 18.2 versions prior to 18.2R3; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R1-S7, 18.4R2; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S4, 19.2R2. **CVE ID : CVE-2020-1688**		
ex4300					
N/A	16-Oct-20	4.3	On Juniper Networks Junos OS devices configured as a DHCP forwarder, the Juniper Networks Dynamic Host Configuration Protocol Daemon (jdhcp) process	https://kb.juniper.net/JSA11056	H-JUN-EX43-031120/1663

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			might crash when receiving a malformed DHCP packet. This issue only affects devices configured as DHCP forwarder with forward-only option, that forward specified DHCP client packets, without creating a new subscriber session. The jdhcpd daemon automatically restarts without intervention, but continuous receipt of the malformed DHCP packet will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. This issue can be triggered only by DHCPv4, it cannot be triggered by DHCPv6. This issue affects Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S16; 12.3X48 versions prior to 12.3X48-D105 on SRX Series; 14.1X53 versions prior to 14.1X53-D60 on EX and QFX Series; 15.1 versions prior to 15.1R7-S7; 15.1X49 versions prior to 15.1X49-D221, 15.1X49-D230 on SRX Series; 15.1X53 versions prior to 15.1X53-D593 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S5. **CVE ID : CVE-2020-1661**		
Uncontrolled Resource Consumption	16-Oct-20	3.3	On Juniper Networks EX4300 Series, receipt of a stream of specific IPv4 packets can cause Routing Engine (RE) high CPU load, which could lead to network protocol	N/A	H-JUN-EX43-031120/1664

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operation issue and traffic interruption. This specific packets can originate only from within the broadcast domain where the device is connected. This issue occurs when the packets enter to the IRB interface. Only IPv4 packets can trigger this issue. IPv6 packets cannot trigger this issue. This issue affects Juniper Networks Junos OS on EX4300 series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.1 versions prior to 18.1R3-S10; 18.2 versions prior to 18.2R3-S4; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2; 18.4 versions prior to 18.4R2-S4, 18.4R3-S2; 19.1 versions prior to 19.1R2-S2, 19.1R3-S1; 19.2 versions prior to 19.2R1-S5, 19.2R2-S1, 19.2R3; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2; 20.1 versions prior to 20.1R1-S3, 20.1R2. **CVE ID : CVE-2020-1670**		
ex4600					
N/A	16-Oct-20	4.3	On Juniper Networks Junos OS devices configured as a DHCP forwarder, the Juniper Networks Dynamic Host Configuration Protocol Daemon (jdhcp) process might crash when receiving a	https://kb.juniper.net/JSA11056	H-JUN-EX46-031120/1665

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malformed DHCP packet. This issue only affects devices configured as DHCP forwarder with forward-only option, that forward specified DHCP client packets, without creating a new subscriber session. The jdhcpd daemon automatically restarts without intervention, but continuous receipt of the malformed DHCP packet will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. This issue can be triggered only by DHCPv4, it cannot be triggered by DHCPv6. This issue affects Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S16; 12.3X48 versions prior to 12.3X48-D105 on SRX Series; 14.1X53 versions prior to 14.1X53-D60 on EX and QFX Series; 15.1 versions prior to 15.1R7-S7; 15.1X49 versions prior to 15.1X49-D221, 15.1X49-D230 on SRX Series; 15.1X53 versions prior to 15.1X53-D593 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S5. **CVE ID : CVE-2020-1661**		
qfx5100					
N/A	16-Oct-20	4.3	On Juniper Networks Junos OS devices configured as a DHCP forwarder, the Juniper Networks Dynamic Host Configuration Protocol	https://kb.juniper.net/JSA11056	H-JUN-QFX5-031120/1666

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Daemon (jdhcp) process might crash when receiving a malformed DHCP packet. This issue only affects devices configured as DHCP forwarder with forward-only option, that forward specified DHCP client packets, without creating a new subscriber session. The jdhcpd daemon automatically restarts without intervention, but continuous receipt of the malformed DHCP packet will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. This issue can be triggered only by DHCPv4, it cannot be triggered by DHCPv6. This issue affects Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S16; 12.3X48 versions prior to 12.3X48-D105 on SRX Series; 14.1X53 versions prior to 14.1X53-D60 on EX and QFX Series; 15.1 versions prior to 15.1R7-S7; 15.1X49 versions prior to 15.1X49-D221, 15.1X49-D230 on SRX Series; 15.1X53 versions prior to 15.1X53-D593 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S5. **CVE ID : CVE-2020-1661**		
N/A	16-Oct-20	4.3	On Juniper Networks PTX and QFX Series devices with packet sampling configured using tunnel-observation mpls-over-udp, sampling of a	https://kb.juniper.net/JSA11076	H-JUN-QFX5-031120/1667

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malformed packet can cause the Kernel Routing Table (KRT) queue to become stuck. KRT is the module within the Routing Process Daemon (RPD) that synchronized the routing tables with the forwarding tables in the kernel. This table is then synchronized to the Packet Forwarding Engine (PFE) via the KRT queue. Thus, when KRT queue become stuck, it can lead to unexpected packet forwarding issues. An administrator can monitor the following command to check if there is the KRT queue is stuck: user@device > show krt state ... Number of async queue entries: 65007 <--- this value keep on increasing. When this issue occurs, the following message might appear in the /var/log/messages: DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Too many delayed route/nexthop unrefs. Op 2 err 55, rtsm_id 5:-1, msg type 2 DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Memory usage of M_RTNEXTHOP type = (0) Max size possible for M_RTNEXTHOP type = (7297134592) Current delayed unref = (60000), Current unique delayed unref = (18420), Max delayed unref		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on this platform = (40000) Current delayed weight unref = (60000) Max delayed weight unref on this platform= (400000) curproc = rpd This issue affects Juniper Networks Junos OS on PTX/QFX Series: 17.2X75 versions prior to 17.2X75-D105; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.2X75 versions prior to 18.2X75-D420, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R1-S7, 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R2-S2, 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2. This issue does not affect Juniper Networks Junos OS prior to 18.1R1. **CVE ID : CVE-2020-1679**		
Information Exposure Through Discrepancy	16-Oct-20	5	When configuring stateless firewall filters in Juniper Networks EX4600 and QFX 5000 Series devices using Virtual Extensible LAN protocol (VXLAN), the discard action will fail to discard traffic under certain conditions. Given a firewall filter configuration similar to: family ethernet-switching {	https://kb.juniper.net/JSA11082	H-JUN-QFX5-031120/1668

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			filter L2-VLAN { term ALLOW { from { user-vlan-id 100; } then { accept; } } term NON-MATCH { then { discard; } } when there is only one term containing a 'user-vlan-id' match condition, and no other terms in the firewall filter except discard, the discard action for non-matching traffic will only discard traffic with the same VLAN ID specified under 'user-vlan-id'. Other traffic (e.g. VLAN ID 200) will not be discarded. This unexpected behavior can lead to unintended traffic passing through the interface where the firewall filter is applied. This issue only affects systems using VXLANs. This issue affects Juniper Networks Junos OS on QFX5K Series: 18.1 versions prior to 18.1R3-S7, except 18.1R3; 18.2 versions prior to 18.2R2-S7, 18.2R3-S1; 18.3 versions prior to 18.3R1-S5, 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R1-S7, 18.4R2-S1, 18.4R3; 19.1 versions prior to 19.1R1-S5, 19.1R2; 19.2 versions prior to 19.2R1-S5, 19.2R2. **CVE ID : CVE-2020-1685**		
Uncontrolled Resource Consumption	16-Oct-20	3.3	On Juniper Networks EX4300-MP Series, EX4600 Series and QFX5K Series deployed in a Virtual Chassis configuration, receipt of a	https://kb.juniper.net/JSA11086	H-JUN-QFX5-031120/1669

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			stream of specific layer 2 frames can cause high CPU load, which could lead to traffic interruption. This issue does not occur when the device is deployed in Stand Alone configuration. The offending layer 2 frame packets can originate only from within the broadcast domain where the device is connected. This issue affects Juniper Networks Junos OS on EX4300-MP Series, EX4600 Series and QFX5K Series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S3, 20.1R2. **CVE ID : CVE-2020-1689**		
ex2300					
N/A	16-Oct-20	4.3	On Juniper Networks Junos OS devices configured as a DHCP forwarder, the Juniper Networks Dynamic Host Configuration Protocol	https://kb.juniper.net/JSA11056	H-JUN-EX23-031120/1670

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Daemon (jdhcp) process might crash when receiving a malformed DHCP packet. This issue only affects devices configured as DHCP forwarder with forward-only option, that forward specified DHCP client packets, without creating a new subscriber session. The jdhcpd daemon automatically restarts without intervention, but continuous receipt of the malformed DHCP packet will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. This issue can be triggered only by DHCPv4, it cannot be triggered by DHCPv6. This issue affects Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S16; 12.3X48 versions prior to 12.3X48-D105 on SRX Series; 14.1X53 versions prior to 14.1X53-D60 on EX and QFX Series; 15.1 versions prior to 15.1R7-S7; 15.1X49 versions prior to 15.1X49-D221, 15.1X49-D230 on SRX Series; 15.1X53 versions prior to 15.1X53-D593 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S5. **CVE ID : CVE-2020-1661**		
Uncontrolled Resource Consumption	16-Oct-20	3.3	On Juniper Networks EX2300 Series, receipt of a stream of specific multicast packets by the layer2 interface can cause high CPU load, which could	https://kb.juniper.net/JSA11065	H-JUN-EX23-031120/1671

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to traffic interruption. This issue occurs when multicast packets are received by the layer 2 interface. To check if the device has high CPU load due to this issue, the administrator can issue the following command: user@host> show chassis routing-engine Routing Engine status: ... Idle 2 percent the "Idle" value shows as low (2 % in the example above), and also the following command: user@host> show system processes summary ... PID USERNAME PRI NICE SIZE RES STATE TIME WCPU COMMAND 11639 root 52 0 283M 11296K select 12:15 44.97% eventd 11803 root 81 0 719M 239M RUN 251:12 31.98% fxpc{fxpc} the eventd and the fxpc processes might use higher WCPU percentage (respectively 44.97% and 31.98% in the above example). This issue affects Juniper Networks Junos OS on EX2300 Series: 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2. **CVE ID : CVE-2020-1668**		
ex3400					
N/A	16-Oct-20	4.3	On Juniper Networks Junos OS devices configured as a DHCP forwarder, the Juniper Networks Dynamic Host Configuration Protocol Daemon (jdhcp) process might crash when receiving a malformed DHCP packet. This issue only affects devices configured as DHCP forwarder with forward-only option, that forward specified DHCP client packets, without creating a new subscriber session. The jdhcpd daemon automatically restarts without intervention, but continuous receipt of the malformed DHCP packet will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. This issue can be triggered only by DHCPv4, it cannot be triggered by DHCPv6. This issue affects Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S16; 12.3X48 versions prior to 12.3X48-D105 on SRX Series; 14.1X53 versions prior to 14.1X53-D60 on EX and QFX Series; 15.1 versions	https://kb.juniper.net/JSA11056	H-JUN-EX34-031120/1672

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 15.1R7-S7; 15.1X49 versions prior to 15.1X49-D221, 15.1X49-D230 on SRX Series; 15.1X53 versions prior to 15.1X53-D593 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S5. **CVE ID : CVE-2020-1661**		
ex2300-c					
N/A	16-Oct-20	4.3	On Juniper Networks Junos OS devices configured as a DHCP forwarder, the Juniper Networks Dynamic Host Configuration Protocol Daemon (jdhcp) process might crash when receiving a malformed DHCP packet. This issue only affects devices configured as DHCP forwarder with forward-only option, that forward specified DHCP client packets, without creating a new subscriber session. The jdhcpd daemon automatically restarts without intervention, but continuous receipt of the malformed DHCP packet will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. This issue can be triggered only by DHCPv4, it cannot be triggered by DHCPv6. This issue affects Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S16; 12.3X48 versions prior to 12.3X48-D105 on SRX Series; 14.1X53 versions	https://kb.juniper.net/JSA11056	H-JUN-EX23-031120/1673

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 14.1X53-D60 on EX and QFX Series; 15.1 versions prior to 15.1R7-S7; 15.1X49 versions prior to 15.1X49-D221, 15.1X49-D230 on SRX Series; 15.1X53 versions prior to 15.1X53-D593 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S5. **CVE ID : CVE-2020-1661**		
ex4650					
N/A	16-Oct-20	4.3	On Juniper Networks Junos OS devices configured as a DHCP forwarder, the Juniper Networks Dynamic Host Configuration Protocol Daemon (jdhcp) process might crash when receiving a malformed DHCP packet. This issue only affects devices configured as DHCP forwarder with forward-only option, that forward specified DHCP client packets, without creating a new subscriber session. The jdhcpd daemon automatically restarts without intervention, but continuous receipt of the malformed DHCP packet will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. This issue can be triggered only by DHCPv4, it cannot be triggered by DHCPv6. This issue affects Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S16; 12.3X48 versions prior	https://kb.juniper.net/JSA11056	H-JUN-EX46-031120/1674

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to 12.3X48-D105 on SRX Series; 14.1X53 versions prior to 14.1X53-D60 on EX and QFX Series; 15.1 versions prior to 15.1R7-S7; 15.1X49 versions prior to 15.1X49-D221, 15.1X49-D230 on SRX Series; 15.1X53 versions prior to 15.1X53-D593 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S5. **CVE ID : CVE-2020-1661**		
qfx5110					
N/A	16-Oct-20	4.3	On Juniper Networks Junos OS devices configured as a DHCP forwarder, the Juniper Networks Dynamic Host Configuration Protocol Daemon (jdhcp) process might crash when receiving a malformed DHCP packet. This issue only affects devices configured as DHCP forwarder with forward-only option, that forward specified DHCP client packets, without creating a new subscriber session. The jdhcpd daemon automatically restarts without intervention, but continuous receipt of the malformed DHCP packet will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. This issue can be triggered only by DHCPv4, it cannot be triggered by DHCPv6. This issue affects Juniper Networks Junos OS: 12.3	https://kb.juniper.net/JSA11056	H-JUN-QFX5-031120/1675

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 12.3R12-S16; 12.3X48 versions prior to 12.3X48-D105 on SRX Series; 14.1X53 versions prior to 14.1X53-D60 on EX and QFX Series; 15.1 versions prior to 15.1R7-S7; 15.1X49 versions prior to 15.1X49-D221, 15.1X49-D230 on SRX Series; 15.1X53 versions prior to 15.1X53-D593 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S5. **CVE ID : CVE-2020-1661**		
N/A	16-Oct-20	4.3	On Juniper Networks PTX and QFX Series devices with packet sampling configured using tunnel-observation mpls-over-udp, sampling of a malformed packet can cause the Kernel Routing Table (KRT) queue to become stuck. KRT is the module within the Routing Process Daemon (RPD) that synchronized the routing tables with the forwarding tables in the kernel. This table is then synchronized to the Packet Forwarding Engine (PFE) via the KRT queue. Thus, when KRT queue become stuck, it can lead to unexpected packet forwarding issues. An administrator can monitor the following command to check if there is the KRT queue is stuck: user@device > show krt state ... Number of async queue entries: 65007	https://kb.juniper.net/JSA11076	H-JUN-QFX5-031120/1676

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<--- this value keep on increasing. When this issue occurs, the following message might appear in the /var/log/messages: DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Too many delayed route/nexthop unrefs. Op 2 err 55, rtsm_id 5:-1, msg type 2 DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Memory usage of M_RTNEXTHOP type = (0) Max size possible for M_RTNEXTHOP type = (7297134592) Current delayed unref = (60000), Current unique delayed unref = (18420), Max delayed unref on this platform = (40000) Current delayed weight unref = (60000) Max delayed weight unref on this platform= (400000) curproc = rpd This issue affects Juniper Networks Junos OS on PTX/QFX Series: 17.2X75 versions prior to 17.2X75-D105; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.2X75 versions prior to 18.2X75-D420, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R1-S7, 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R2-S2, 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2. This issue does not affect Juniper Networks Junos OS prior to 18.1R1. **CVE ID : CVE-2020-1679**		
Information Exposure Through Discrepancy	16-Oct-20	5	When configuring stateless firewall filters in Juniper Networks EX4600 and QFX 5000 Series devices using Virtual Extensible LAN protocol (VXLAN), the discard action will fail to discard traffic under certain conditions. Given a firewall filter configuration similar to: family ethernet-switching { filter L2-VLAN { term ALLOW { from { user-vlan-id 100; } then { accept; } } term NON-MATCH { then { discard; } } when there is only one term containing a 'user-vlan-id' match condition, and no other terms in the firewall filter except discard, the discard action for non-matching traffic will only discard traffic with the same VLAN ID specified under 'user-vlan-id'. Other traffic (e.g. VLAN ID 200) will not be discarded. This unexpected behavior can lead to unintended traffic passing through the interface where the firewall filter is applied. This issue only affects systems using VXLANs. This	https://kb.juniper.net/JSA11082	H-JUN-QFX5-031120/1677

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue affects Juniper Networks Junos OS on QFX5K Series: 18.1 versions prior to 18.1R3-S7, except 18.1R3; 18.2 versions prior to 18.2R2-S7, 18.2R3-S1; 18.3 versions prior to 18.3R1-S5, 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R1-S7, 18.4R2-S1, 18.4R3; 19.1 versions prior to 19.1R1-S5, 19.1R2; 19.2 versions prior to 19.2R1-S5, 19.2R2. **CVE ID : CVE-2020-1685**		
qfx5120					
N/A	16-Oct-20	4.3	On Juniper Networks Junos OS devices configured as a DHCP forwarder, the Juniper Networks Dynamic Host Configuration Protocol Daemon (jdhcp) process might crash when receiving a malformed DHCP packet. This issue only affects devices configured as DHCP forwarder with forward-only option, that forward specified DHCP client packets, without creating a new subscriber session. The jdhcpd daemon automatically restarts without intervention, but continuous receipt of the malformed DHCP packet will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. This issue can be triggered only by DHCPv4, it cannot be triggered by DHCPv6. This	https://kb.juniper.net/JSA11056	H-JUN-QFX5-031120/1678

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue affects Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S16; 12.3X48 versions prior to 12.3X48-D105 on SRX Series; 14.1X53 versions prior to 14.1X53-D60 on EX and QFX Series; 15.1 versions prior to 15.1R7-S7; 15.1X49 versions prior to 15.1X49-D221, 15.1X49-D230 on SRX Series; 15.1X53 versions prior to 15.1X53-D593 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S5. **CVE ID : CVE-2020-1661**		
N/A	16-Oct-20	4.3	On Juniper Networks PTX and QFX Series devices with packet sampling configured using tunnel-observation mpls-over-udp, sampling of a malformed packet can cause the Kernel Routing Table (KRT) queue to become stuck. KRT is the module within the Routing Process Daemon (RPD) that synchronized the routing tables with the forwarding tables in the kernel. This table is then synchronized to the Packet Forwarding Engine (PFE) via the KRT queue. Thus, when KRT queue become stuck, it can lead to unexpected packet forwarding issues. An administrator can monitor the following command to check if there is the KRT queue is stuck: user@device	https://kb.juniper.net/JSA11076	H-JUN-QFX5-031120/1679

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			> show krt state ... Number of async queue entries: 65007 <--- this value keep on increasing. When this issue occurs, the following message might appear in the /var/log/messages: DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Too many delayed route/nexthop unrefs. Op 2 err 55, rtsm_id 5:-1, msg type 2 DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Memory usage of M_RTNEXTHOP type = (0) Max size possible for M_RTNEXTHOP type = (7297134592) Current delayed unref = (60000), Current unique delayed unref = (18420), Max delayed unref on this platform = (40000) Current delayed weight unref = (60000) Max delayed weight unref on this platform= (400000) curproc = rpd This issue affects Juniper Networks Junos OS on PTX/QFX Series: 17.2X75 versions prior to 17.2X75-D105; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.2X75 versions prior to 18.2X75-D420, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R1-S7, 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R2-S2, 19.1R3-S2; 19.2 versions		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2. This issue does not affect Juniper Networks Junos OS prior to 18.1R1. **CVE ID : CVE-2020-1679**		
Information Exposure Through Discrepancy	16-Oct-20	5	When configuring stateless firewall filters in Juniper Networks EX4600 and QFX 5000 Series devices using Virtual Extensible LAN protocol (VXLAN), the discard action will fail to discard traffic under certain conditions. Given a firewall filter configuration similar to: family ethernet-switching { filter L2-VLAN { term ALLOW { from { user-vlan-id 100; } then { accept; } } term NON-MATCH { then { discard; } } when there is only one term containing a 'user-vlan-id' match condition, and no other terms in the firewall filter except discard, the discard action for non-matching traffic will only discard traffic with the same VLAN ID specified under 'user-vlan-id'. Other traffic (e.g. VLAN ID 200) will not be discarded. This unexpected behavior can lead to unintended traffic passing through the interface where the firewall filter is applied.	https://kb.juniper.net/JSA11082	H-JUN-QFX5-031120/1680

CVSS Scoring Scale	0-1	1-2	2-3	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 issue only affects systems using VXLANs. This issue affects Juniper Networks Junos OS on QFX5K Series: 18.1 versions prior to 18.1R3-S7, except 18.1R3; 18.2 versions prior to 18.2R2-S7, 18.2R3-S1; 18.3 versions prior to 18.3R1-S5, 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R1-S7, 18.4R2-S1, 18.4R3; 19.1 versions prior to 19.1R1-S5, 19.1R2; 19.2 versions prior to 19.2R1-S5, 19.2R2. **CVE ID : CVE-2020-1685**		
Uncontrolled Resource Consumption	16-Oct-20	3.3	On Juniper Networks EX4300-MP Series, EX4600 Series and QFX5K Series deployed in a Virtual Chassis configuration, receipt of a stream of specific layer 2 frames can cause high CPU load, which could lead to traffic interruption. This issue does not occur when the device is deployed in Stand Alone configuration. The offending layer 2 frame packets can originate only from within the broadcast domain where the device is connected. This issue affects Juniper Networks Junos OS on EX4300-MP Series, EX4600 Series and QFX5K Series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2	https://kb.juniper.net/JSA11086	H-JUN-QFX5-031120/1681

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S3, 20.1R2. **CVE ID : CVE-2020-1689**		
qfx5200					
N/A	16-Oct-20	4.3	On Juniper Networks Junos OS devices configured as a DHCP forwarder, the Juniper Networks Dynamic Host Configuration Protocol Daemon (jdhcp) process might crash when receiving a malformed DHCP packet. This issue only affects devices configured as DHCP forwarder with forward-only option, that forward specified DHCP client packets, without creating a new subscriber session. The jdhcpd daemon automatically restarts without intervention, but continuous receipt of the malformed DHCP packet will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. This issue can be triggered only by DHCPv4, it cannot be triggered by DHCPv6. This	https://kb.juniper.net/JSA11056	H-JUN-QFX5-031120/1682

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue affects Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S16; 12.3X48 versions prior to 12.3X48-D105 on SRX Series; 14.1X53 versions prior to 14.1X53-D60 on EX and QFX Series; 15.1 versions prior to 15.1R7-S7; 15.1X49 versions prior to 15.1X49-D221, 15.1X49-D230 on SRX Series; 15.1X53 versions prior to 15.1X53-D593 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S5. **CVE ID : CVE-2020-1661**		
N/A	16-Oct-20	4.3	On Juniper Networks PTX and QFX Series devices with packet sampling configured using tunnel-observation mpls-over-udp, sampling of a malformed packet can cause the Kernel Routing Table (KRT) queue to become stuck. KRT is the module within the Routing Process Daemon (RPD) that synchronized the routing tables with the forwarding tables in the kernel. This table is then synchronized to the Packet Forwarding Engine (PFE) via the KRT queue. Thus, when KRT queue become stuck, it can lead to unexpected packet forwarding issues. An administrator can monitor the following command to check if there is the KRT queue is stuck: user@device	https://kb.juniper.net/JSA11076	H-JUN-QFX5-031120/1683

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			> show krt state ... Number of async queue entries: 65007 <--- this value keep on increasing. When this issue occurs, the following message might appear in the /var/log/messages: DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Too many delayed route/nexthop unrefs. Op 2 err 55, rtsm_id 5:-1, msg type 2 DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Memory usage of M_RTNEXTHOP type = (0) Max size possible for M_RTNEXTHOP type = (7297134592) Current delayed unref = (60000), Current unique delayed unref = (18420), Max delayed unref on this platform = (40000) Current delayed weight unref = (60000) Max delayed weight unref on this platform= (400000) curproc = rpd This issue affects Juniper Networks Junos OS on PTX/QFX Series: 17.2X75 versions prior to 17.2X75-D105; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.2X75 versions prior to 18.2X75-D420, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R1-S7, 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R2-S2, 19.1R3-S2; 19.2 versions		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2. This issue does not affect Juniper Networks Junos OS prior to 18.1R1. **CVE ID : CVE-2020-1679**		
Information Exposure Through Discrepancy	16-Oct-20	5	When configuring stateless firewall filters in Juniper Networks EX4600 and QFX 5000 Series devices using Virtual Extensible LAN protocol (VXLAN), the discard action will fail to discard traffic under certain conditions. Given a firewall filter configuration similar to: family ethernet-switching { filter L2-VLAN { term ALLOW { from { user-vlan-id 100; } then { accept; } } term NON-MATCH { then { discard; } } when there is only one term containing a 'user-vlan-id' match condition, and no other terms in the firewall filter except discard, the discard action for non-matching traffic will only discard traffic with the same VLAN ID specified under 'user-vlan-id'. Other traffic (e.g. VLAN ID 200) will not be discarded. This unexpected behavior can lead to unintended traffic passing through the interface where the firewall filter is applied.	https://kb.juniper.net/JSA11082	H-JUN-QFX5-031120/1684

CVSS Scoring Scale	0-1	1-2	2-3	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 issue only affects systems using VXLANs. This issue affects Juniper Networks Junos OS on QFX5K Series: 18.1 versions prior to 18.1R3-S7, except 18.1R3; 18.2 versions prior to 18.2R2-S7, 18.2R3-S1; 18.3 versions prior to 18.3R1-S5, 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R1-S7, 18.4R2-S1, 18.4R3; 19.1 versions prior to 19.1R1-S5, 19.1R2; 19.2 versions prior to 19.2R1-S5, 19.2R2. **CVE ID : CVE-2020-1685**		
Uncontrolled Resource Consumption	16-Oct-20	3.3	On Juniper Networks EX4300-MP Series, EX4600 Series and QFX5K Series deployed in a Virtual Chassis configuration, receipt of a stream of specific layer 2 frames can cause high CPU load, which could lead to traffic interruption. This issue does not occur when the device is deployed in Stand Alone configuration. The offending layer 2 frame packets can originate only from within the broadcast domain where the device is connected. This issue affects Juniper Networks Junos OS on EX4300-MP Series, EX4600 Series and QFX5K Series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2, 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2	https://kb.juniper.net/JSA11086	H-JUN-QFX5-031120/1685

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S3, 20.1R2. **CVE ID : CVE-2020-1689**		
qfx5210					
N/A	16-Oct-20	4.3	On Juniper Networks Junos OS devices configured as a DHCP forwarder, the Juniper Networks Dynamic Host Configuration Protocol Daemon (jdhcp) process might crash when receiving a malformed DHCP packet. This issue only affects devices configured as DHCP forwarder with forward-only option, that forward specified DHCP client packets, without creating a new subscriber session. The jdhcpd daemon automatically restarts without intervention, but continuous receipt of the malformed DHCP packet will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. This issue can be triggered only by DHCPv4, it cannot be triggered by DHCPv6. This	https://kb.juniper.net/JSA11056	H-JUN-QFX5-031120/1686

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue affects Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S16; 12.3X48 versions prior to 12.3X48-D105 on SRX Series; 14.1X53 versions prior to 14.1X53-D60 on EX and QFX Series; 15.1 versions prior to 15.1R7-S7; 15.1X49 versions prior to 15.1X49-D221, 15.1X49-D230 on SRX Series; 15.1X53 versions prior to 15.1X53-D593 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S5. **CVE ID : CVE-2020-1661**		
N/A	16-Oct-20	4.3	On Juniper Networks PTX and QFX Series devices with packet sampling configured using tunnel-observation mpls-over-udp, sampling of a malformed packet can cause the Kernel Routing Table (KRT) queue to become stuck. KRT is the module within the Routing Process Daemon (RPD) that synchronized the routing tables with the forwarding tables in the kernel. This table is then synchronized to the Packet Forwarding Engine (PFE) via the KRT queue. Thus, when KRT queue become stuck, it can lead to unexpected packet forwarding issues. An administrator can monitor the following command to check if there is the KRT queue is stuck: user@device	https://kb.juniper.net/JSA11076	H-JUN-QFX5-031120/1687

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			> show krt state ... Number of async queue entries: 65007 <--- this value keep on increasing. When this issue occurs, the following message might appear in the /var/log/messages: DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Too many delayed route/nexthop unrefs. Op 2 err 55, rtsm_id 5:-1, msg type 2 DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Memory usage of M_RTNEXTHOP type = (0) Max size possible for M_RTNEXTHOP type = (7297134592) Current delayed unref = (60000), Current unique delayed unref = (18420), Max delayed unref on this platform = (40000) Current delayed weight unref = (60000) Max delayed weight unref on this platform= (400000) curproc = rpd This issue affects Juniper Networks Junos OS on PTX/QFX Series: 17.2X75 versions prior to 17.2X75-D105; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.2X75 versions prior to 18.2X75-D420, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R1-S7, 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R2-S2, 19.1R3-S2; 19.2 versions		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2. This issue does not affect Juniper Networks Junos OS prior to 18.1R1. **CVE ID : CVE-2020-1679**		
Information Exposure Through Discrepancy	16-Oct-20	5	When configuring stateless firewall filters in Juniper Networks EX4600 and QFX 5000 Series devices using Virtual Extensible LAN protocol (VXLAN), the discard action will fail to discard traffic under certain conditions. Given a firewall filter configuration similar to: family ethernet-switching { filter L2-VLAN { term ALLOW { from { user-vlan-id 100; } then { accept; } } term NON-MATCH { then { discard; } } when there is only one term containing a 'user-vlan-id' match condition, and no other terms in the firewall filter except discard, the discard action for non-matching traffic will only discard traffic with the same VLAN ID specified under 'user-vlan-id'. Other traffic (e.g. VLAN ID 200) will not be discarded. This unexpected behavior can lead to unintended traffic passing through the interface where the firewall filter is applied.	https://kb.juniper.net/JSA11082	H-JUN-QFX5-031120/1688

CVSS Scoring Scale	0-1	1-2	2-3	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 issue only affects systems using VXLANs. This issue affects Juniper Networks Junos OS on QFX5K Series: 18.1 versions prior to 18.1R3-S7, except 18.1R3; 18.2 versions prior to 18.2R2-S7, 18.2R3-S1; 18.3 versions prior to 18.3R1-S5, 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R1-S7, 18.4R2-S1, 18.4R3; 19.1 versions prior to 19.1R1-S5, 19.1R2; 19.2 versions prior to 19.2R1-S5, 19.2R2. **CVE ID : CVE-2020-1685**		
qfx10002					
N/A	16-Oct-20	4.3	On Juniper Networks Junos OS devices configured as a DHCP forwarder, the Juniper Networks Dynamic Host Configuration Protocol Daemon (jdhcp) process might crash when receiving a malformed DHCP packet. This issue only affects devices configured as DHCP forwarder with forward-only option, that forward specified DHCP client packets, without creating a new subscriber session. The jdhcpd daemon automatically restarts without intervention, but continuous receipt of the malformed DHCP packet will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. This issue can be triggered	https://kb.juniper.net/JSA11056	H-JUN-QFX1-031120/1689

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			only by DHCPv4, it cannot be triggered by DHCPv6. This issue affects Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S16; 12.3X48 versions prior to 12.3X48-D105 on SRX Series; 14.1X53 versions prior to 14.1X53-D60 on EX and QFX Series; 15.1 versions prior to 15.1R7-S7; 15.1X49 versions prior to 15.1X49-D221, 15.1X49-D230 on SRX Series; 15.1X53 versions prior to 15.1X53-D593 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S5. **CVE ID : CVE-2020-1661**		
N/A	16-Oct-20	4.3	On Juniper Networks PTX and QFX Series devices with packet sampling configured using tunnel-observation mpls-over-udp, sampling of a malformed packet can cause the Kernel Routing Table (KRT) queue to become stuck. KRT is the module within the Routing Process Daemon (RPD) that synchronized the routing tables with the forwarding tables in the kernel. This table is then synchronized to the Packet Forwarding Engine (PFE) via the KRT queue. Thus, when KRT queue become stuck, it can lead to unexpected packet forwarding issues. An administrator can monitor the following command to	https://kb.juniper.net/JSA11076	H-JUN-QFX1-031120/1690

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check if there is the KRT queue is stuck: user@device > show krt state ... Number of async queue entries: 65007 <--- this value keep on increasing. When this issue occurs, the following message might appear in the /var/log/messages: DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Too many delayed route/nexthop unrefs. Op 2 err 55, rtsm_id 5:-1, msg type 2 DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Memory usage of M_RTNEXTHOP type = (0) Max size possible for M_RTNEXTHOP type = (7297134592) Current delayed unref = (60000), Current unique delayed unref = (18420), Max delayed unref on this platform = (40000) Current delayed weight unref = (60000) Max delayed weight unref on this platform= (400000) curproc = rpd This issue affects Juniper Networks Junos OS on PTX/QFX Series: 17.2X75 versions prior to 17.2X75-D105; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.2X75 versions prior to 18.2X75-D420, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R1-S7, 18.4R2-S5, 18.4R3-S4; 19.1		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 19.1R2-S2, 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2. This issue does not affect Juniper Networks Junos OS prior to 18.1R1. **CVE ID : CVE-2020-1679**		
qfx10008					
N/A	16-Oct-20	4.3	On Juniper Networks Junos OS devices configured as a DHCP forwarder, the Juniper Networks Dynamic Host Configuration Protocol Daemon (jdhcp) process might crash when receiving a malformed DHCP packet. This issue only affects devices configured as DHCP forwarder with forward-only option, that forward specified DHCP client packets, without creating a new subscriber session. The jdhcpd daemon automatically restarts without intervention, but continuous receipt of the malformed DHCP packet will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. This issue can be triggered only by DHCPv4, it cannot be triggered by DHCPv6. This issue affects Juniper Networks Junos OS: 12.3	https://kb.juniper.net/JSA11056	H-JUN-QFX1-031120/1691

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 12.3R12-S16; 12.3X48 versions prior to 12.3X48-D105 on SRX Series; 14.1X53 versions prior to 14.1X53-D60 on EX and QFX Series; 15.1 versions prior to 15.1R7-S7; 15.1X49 versions prior to 15.1X49-D221, 15.1X49-D230 on SRX Series; 15.1X53 versions prior to 15.1X53-D593 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S5. **CVE ID : CVE-2020-1661**		
N/A	16-Oct-20	4.3	On Juniper Networks PTX and QFX Series devices with packet sampling configured using tunnel-observation mpls-over-udp, sampling of a malformed packet can cause the Kernel Routing Table (KRT) queue to become stuck. KRT is the module within the Routing Process Daemon (RPD) that synchronized the routing tables with the forwarding tables in the kernel. This table is then synchronized to the Packet Forwarding Engine (PFE) via the KRT queue. Thus, when KRT queue become stuck, it can lead to unexpected packet forwarding issues. An administrator can monitor the following command to check if there is the KRT queue is stuck: user@device > show krt state ... Number of async queue entries: 65007	https://kb.juniper.net/JSA11076	H-JUN-QFX1-031120/1692

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<--- this value keep on increasing. When this issue occurs, the following message might appear in the /var/log/messages: DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Too many delayed route/nexthop unrefs. Op 2 err 55, rtsm_id 5:-1, msg type 2 DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Memory usage of M_RTNEXTHOP type = (0) Max size possible for M_RTNEXTHOP type = (7297134592) Current delayed unref = (60000), Current unique delayed unref = (18420), Max delayed unref on this platform = (40000) Current delayed weight unref = (60000) Max delayed weight unref on this platform= (400000) curproc = rpd This issue affects Juniper Networks Junos OS on PTX/QFX Series: 17.2X75 versions prior to 17.2X75-D105; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.2X75 versions prior to 18.2X75-D420, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R1-S7, 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R2-S2, 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2. This issue does not affect Juniper Networks Junos OS prior to 18.1R1. **CVE ID : CVE-2020-1679**		
qfx10016					
N/A	16-Oct-20	4.3	On Juniper Networks Junos OS devices configured as a DHCP forwarder, the Juniper Networks Dynamic Host Configuration Protocol Daemon (jdhcp) process might crash when receiving a malformed DHCP packet. This issue only affects devices configured as DHCP forwarder with forward-only option, that forward specified DHCP client packets, without creating a new subscriber session. The jdhcpd daemon automatically restarts without intervention, but continuous receipt of the malformed DHCP packet will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. This issue can be triggered only by DHCPv4, it cannot be triggered by DHCPv6. This issue affects Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S16; 12.3X48 versions prior to 12.3X48-D105 on SRX Series; 14.1X53 versions	https://kb.juniper.net/JSA11056	H-JUN-QFX1-031120/1693

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 14.1X53-D60 on EX and QFX Series; 15.1 versions prior to 15.1R7-S7; 15.1X49 versions prior to 15.1X49-D221, 15.1X49-D230 on SRX Series; 15.1X53 versions prior to 15.1X53-D593 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S5. **CVE ID : CVE-2020-1661**		
N/A	16-Oct-20	4.3	On Juniper Networks PTX and QFX Series devices with packet sampling configured using tunnel-observation mpls-over-udp, sampling of a malformed packet can cause the Kernel Routing Table (KRT) queue to become stuck. KRT is the module within the Routing Process Daemon (RPD) that synchronized the routing tables with the forwarding tables in the kernel. This table is then synchronized to the Packet Forwarding Engine (PFE) via the KRT queue. Thus, when KRT queue become stuck, it can lead to unexpected packet forwarding issues. An administrator can monitor the following command to check if there is the KRT queue is stuck: user@device > show krt state ... Number of async queue entries: 65007 <--- this value keep on increasing. When this issue occurs, the following message might appear in the	https://kb.juniper.net/JSA11076	H-JUN-QFX1-031120/1694

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			/var/log/messages: DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Too many delayed route/nexthop unrefs. Op 2 err 55, rtsm_id 5:-1, msg type 2 DATE DEVICE kernel: %KERN-3: rt_pfe_veto: Memory usage of M_RTNEXTHOP type = (0) Max size possible for M_RTNEXTHOP type = (7297134592) Current delayed unref = (60000), Current unique delayed unref = (18420), Max delayed unref on this platform = (40000) Current delayed weight unref = (60000) Max delayed weight unref on this platform= (400000) curproc = rpd This issue affects Juniper Networks Junos OS on PTX/QFX Series: 17.2X75 versions prior to 17.2X75-D105; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.2X75 versions prior to 18.2X75-D420, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R1-S7, 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R2-S2, 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2,		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.1R2. This issue does not affect Juniper Networks Junos OS prior to 18.1R1. **CVE ID : CVE-2020-1679**		
mx10					
N/A	16-Oct-20	5	On Juniper Networks MX Series and EX9200 Series, in a certain condition the IPv6 Distributed Denial of Service (DDoS) protection might not take affect when it reaches the threshold condition. The DDoS protection allows the device to continue to function while it is under DDoS attack, protecting both the Routing Engine (RE) and the Flexible PIC Concentrator (FPC) during the DDoS attack. When this issue occurs, the RE and/or the FPC can become overwhelmed, which could disrupt network protocol operations and/or interrupt traffic. This issue does not affect IPv4 DDoS protection. This issue affects MX Series and EX9200 Series with Trio-based PFEs (Packet Forwarding Engines). Please refer to https://kb.juniper.net/KB25385 for the list of Trio-based PFEs. This issue affects Juniper Networks Junos OS on MX series and EX9200 Series: 17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110; 17.3 versions	https://kb.juniper.net/JSA11062	H-JUN-MX10-031120/1695

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R2-S7, 18.2R3, 18.2R3-S3; 18.2X75 versions prior to 18.2X75-D30; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2. **CVE ID : CVE-2020-1665**		
Incorrect Calculation of Buffer Size	16-Oct-20	5	On Juniper Networks MX Series with MS-MIC or MS-MPC card configured with NAT64 configuration, receipt of a malformed IPv6 packet may crash the MS-PIC component on MS-MIC or MS-MPC. This issue occurs when a multiservice card is translating the malformed IPv6 packet to IPv4 packet. An unauthenticated attacker can continuously send crafted IPv6 packets through the device causing repetitive MS-PIC process crashes, resulting in an extended Denial of Service condition. This issue affects Juniper Networks Junos OS on MX Series: 15.1 versions prior to 15.1R7-S7; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S6; 17.4 versions prior to 17.4R2-S11, 17.4R3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.2X75 versions prior to 18.2X75-	https://kb.juniper.net/JSA11077	H-JUN-MX10-031120/1696

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			D41, 18.2X75-D430, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2. **CVE ID : CVE-2020-1680**		
mx10003					
N/A	16-Oct-20	5	On Juniper Networks MX Series and EX9200 Series, in a certain condition the IPv6 Distributed Denial of Service (DDoS) protection might not take affect when it reaches the threshold condition. The DDoS protection allows the device to continue to function while it is under DDoS attack, protecting both the Routing Engine (RE) and the Flexible PIC Concentrator (FPC) during the DDoS attack. When this issue occurs, the RE and/or the FPC can become overwhelmed, which could disrupt network protocol operations and/or interrupt traffic. This issue does not affect IPv4 DDoS protection. This issue affects MX Series and EX9200 Series with Trio-based PFEs (Packet Forwarding Engines). Please refer to https://kb.juniper.net/KB25385 for the list of Trio-based PFEs. This issue affects	https://kb.juniper.net/JSA11062	H-JUN-MX10-031120/1697

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Juniper Networks Junos OS on MX series and EX9200 Series: 17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R2-S7, 18.2R3, 18.2R3-S3; 18.2X75 versions prior to 18.2X75-D30; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2. **CVE ID : CVE-2020-1665**		
Incorrect Calculation of Buffer Size	16-Oct-20	5	On Juniper Networks MX Series with MS-MIC or MS-MPC card configured with NAT64 configuration, receipt of a malformed IPv6 packet may crash the MS-PIC component on MS-MIC or MS-MPC. This issue occurs when a multiservice card is translating the malformed IPv6 packet to IPv4 packet. An unauthenticated attacker can continuously send crafted IPv6 packets through the device causing repetitive MS-PIC process crashes, resulting in an extended Denial of Service condition. This issue affects Juniper Networks Junos OS on MX Series: 15.1 versions prior to 15.1R7-S7; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to	https://kb.juniper.net/JSA11077	H-JUN-MX10-031120/1698

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			17.3R3-S6; 17.4 versions prior to 17.4R2-S11, 17.4R3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D430, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2. **CVE ID : CVE-2020-1680**		
mx104					
N/A	16-Oct-20	5	On Juniper Networks MX Series and EX9200 Series, in a certain condition the IPv6 Distributed Denial of Service (DDoS) protection might not take affect when it reaches the threshold condition. The DDoS protection allows the device to continue to function while it is under DDoS attack, protecting both the Routing Engine (RE) and the Flexible PIC Concentrator (FPC) during the DDoS attack. When this issue occurs, the RE and/or the FPC can become overwhelmed, which could disrupt network protocol operations and/or interrupt traffic. This issue does not affect IPv4 DDoS protection. This issue affects MX Series and EX9200 Series	https://kb.juniper.net/JSA11062	H-JUN-MX10-031120/1699

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with Trio-based PFEs (Packet Forwarding Engines). Please refer to https://kb.juniper.net/KB25385 for the list of Trio-based PFEs. This issue affects Juniper Networks Junos OS on MX series and EX9200 Series: 17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R2-S7, 18.2R3, 18.2R3-S3; 18.2X75 versions prior to 18.2X75-D30; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2. **CVE ID : CVE-2020-1665**		
Incorrect Calculation of Buffer Size	16-Oct-20	5	On Juniper Networks MX Series with MS-MIC or MS-MPC card configured with NAT64 configuration, receipt of a malformed IPv6 packet may crash the MS-PIC component on MS-MIC or MS-MPC. This issue occurs when a multiservice card is translating the malformed IPv6 packet to IPv4 packet. An unauthenticated attacker can continuously send crafted IPv6 packets through the device causing repetitive MS-PIC process crashes, resulting in an extended Denial of Service condition. This issue affects Juniper Networks Junos OS on MX Series: 15.1	https://kb.juniper.net/JSA11077	H-JUN-MX10-031120/1700

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 15.1R7-S7; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S6; 17.4 versions prior to 17.4R2-S11, 17.4R3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D430, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2. **CVE ID : CVE-2020-1680**		
mx150					
N/A	16-Oct-20	5	On Juniper Networks MX Series and EX9200 Series, in a certain condition the IPv6 Distributed Denial of Service (DDoS) protection might not take affect when it reaches the threshold condition. The DDoS protection allows the device to continue to function while it is under DDoS attack, protecting both the Routing Engine (RE) and the Flexible PIC Concentrator (FPC) during the DDoS attack. When this issue occurs, the RE and/or the FPC can become overwhelmed, which	https://kb.juniper.net/JSA11062	H-JUN-MX15-031120/1701

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could disrupt network protocol operations and/or interrupt traffic. This issue does not affect IPv4 DDoS protection. This issue affects MX Series and EX9200 Series with Trio-based PFEs (Packet Forwarding Engines). Please refer to https://kb.juniper.net/KB25385 for the list of Trio-based PFEs. This issue affects Juniper Networks Junos OS on MX series and EX9200 Series: 17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R2-S7, 18.2R3, 18.2R3-S3; 18.2X75 versions prior to 18.2X75-D30; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2. **CVE ID : CVE-2020-1665**		
Incorrect Calculation of Buffer Size	16-Oct-20	5	On Juniper Networks MX Series with MS-MIC or MS-MPC card configured with NAT64 configuration, receipt of a malformed IPv6 packet may crash the MS-PIC component on MS-MIC or MS-MPC. This issue occurs when a multiservice card is translating the malformed IPv6 packet to IPv4 packet. An unauthenticated attacker can continuously send crafted IPv6 packets through the	https://kb.juniper.net/JSA11077	H-JUN-MX15-031120/1702

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device causing repetitive MS-PIC process crashes, resulting in an extended Denial of Service condition. This issue affects Juniper Networks Junos OS on MX Series: 15.1 versions prior to 15.1R7-S7; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S6; 17.4 versions prior to 17.4R2-S11, 17.4R3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D430, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2. **CVE ID : CVE-2020-1680**		
mx2008					
N/A	16-Oct-20	5	On Juniper Networks MX Series and EX9200 Series, in a certain condition the IPv6 Distributed Denial of Service (DDoS) protection might not take affect when it reaches the threshold condition. The DDoS protection allows the device to continue to function while it is under DDoS attack, protecting both the Routing	https://kb.juniper.net/JSA11062	H-JUN-MX20-031120/1703

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Engine (RE) and the Flexible PIC Concentrator (FPC) during the DDoS attack. When this issue occurs, the RE and/or the FPC can become overwhelmed, which could disrupt network protocol operations and/or interrupt traffic. This issue does not affect IPv4 DDoS protection. This issue affects MX Series and EX9200 Series with Trio-based PFEs (Packet Forwarding Engines). Please refer to https://kb.juniper.net/KB25385 for the list of Trio-based PFEs. This issue affects Juniper Networks Junos OS on MX series and EX9200 Series: 17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R2-S7, 18.2R3, 18.2R3-S3; 18.2X75 versions prior to 18.2X75-D30; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2. **CVE ID : CVE-2020-1665**		
Incorrect Calculation of Buffer Size	16-Oct-20	5	On Juniper Networks MX Series with MS-MIC or MS-MPC card configured with NAT64 configuration, receipt of a malformed IPv6 packet may crash the MS-PIC component on MS-MIC or MS-MPC. This issue occurs when	https://kb.juniper.net/JSA11077	H-JUN-MX20-031120/1704

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a multiservice card is translating the malformed IPv6 packet to IPv4 packet. An unauthenticated attacker can continuously send crafted IPv6 packets through the device causing repetitive MS-PIC process crashes, resulting in an extended Denial of Service condition. This issue affects Juniper Networks Junos OS on MX Series: 15.1 versions prior to 15.1R7-S7; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S6; 17.4 versions prior to 17.4R2-S11, 17.4R3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D430, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2. **CVE ID : CVE-2020-1680**		
mx2010					
N/A	16-Oct-20	5	On Juniper Networks MX Series and EX9200 Series, in a certain condition the IPv6 Distributed Denial of Service (DDoS) protection might not	https://kb.juniper.net/JSA11062	H-JUN-MX20-031120/1705

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			take affect when it reaches the threshold condition. The DDoS protection allows the device to continue to function while it is under DDoS attack, protecting both the Routing Engine (RE) and the Flexible PIC Concentrator (FPC) during the DDoS attack. When this issue occurs, the RE and/or the FPC can become overwhelmed, which could disrupt network protocol operations and/or interrupt traffic. This issue does not affect IPv4 DDoS protection. This issue affects MX Series and EX9200 Series with Trio-based PFEs (Packet Forwarding Engines). Please refer to https://kb.juniper.net/KB25385 for the list of Trio-based PFEs. This issue affects Juniper Networks Junos OS on MX series and EX9200 Series: 17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R2-S7, 18.2R3, 18.2R3-S3; 18.2X75 versions prior to 18.2X75-D30; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2. **CVE ID : CVE-2020-1665**		
Incorrect Calculation	16-Oct-20	5	On Juniper Networks MX Series with MS-MIC or MS-	https://kb.juniper.net/JS	H-JUN-MX20-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Buffer Size			MPC card configured with NAT64 configuration, receipt of a malformed IPv6 packet may crash the MS-PIC component on MS-MIC or MS-MPC. This issue occurs when a multiservice card is translating the malformed IPv6 packet to IPv4 packet. An unauthenticated attacker can continuously send crafted IPv6 packets through the device causing repetitive MS-PIC process crashes, resulting in an extended Denial of Service condition. This issue affects Juniper Networks Junos OS on MX Series: 15.1 versions prior to 15.1R7-S7; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S8; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S6; 17.4 versions prior to 17.4R2-S11, 17.4R3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D430, 18.2X75-D53, 18.2X75-D65; 18.3 versions prior to 18.3R2-S4, 18.3R3; 18.4 versions prior to 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2. **CVE ID : CVE-2020-1680**	A11077	031120/1706

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
Oracle					
hospitality_res_3700					
N/A	21-Oct-20	5	Vulnerability in the Oracle Hospitality RES 3700 product of Oracle Food and Beverage Applications (component: CAL). The supported version that is affected is 5.7. Easily exploitable vulnerability allows unauthenticated attacker with network access via TCP to compromise Oracle Hospitality RES 3700. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hospitality RES 3700 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-2020-14783**	N/A	H-ORA-HOSP-031120/1707
reason					
s2020					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-20	4.3	The affected Reason S20 Ethernet Switch is vulnerable to cross-site scripting (XSS), which may allow attackers to trick users into following a link or navigating to a page that posts a malicious JavaScript statement to the vulnerable site, causing the malicious JavaScript to be rendered by the site and executed by the victim client. **CVE ID : CVE-2020-16246**	N/A	H-REA-S202-031120/1708

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
s2024					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Oct-20	4.3	The affected Reason S20 Ethernet Switch is vulnerable to cross-site scripting (XSS), which may allow attackers to trick users into following a link or navigating to a page that posts a malicious JavaScript statement to the vulnerable site, causing the malicious JavaScript to be rendered by the site and executed by the victim client. **CVE ID : CVE-2020-16246**	N/A	H-REA-S202-031120/1709
Rockwellautomation					
flex_i\/o_1794-aent					
N/A	19-Oct-20	7.8	An exploitable denial of service vulnerability exists in the ENIP Request Path Logical Segment functionality of Allen-Bradley Flex IO 1794-AENT/B 4.003. A specially crafted network request can cause a loss of communications with the device resulting in denial-of-service. An attacker can send a malicious packet to trigger this vulnerability by sending an Electronic Key Segment with less bytes than required by the Key Format Table. **CVE ID : CVE-2020-6084**	N/A	H-ROC-FLEX-031120/1710
Buffer Copy without Checking Size of Input ('Classic Buffer	19-Oct-20	7.8	An exploitable denial of service vulnerability exists in the ENIP Request Path Logical Segment functionality of Allen-Bradley Flex IO 1794-AENT/B 4.003. A	N/A	H-ROC-FLEX-031120/1711

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			specially crafted network request can cause a loss of communications with the device resulting in denial-of-service. An attacker can send a malicious packet to trigger this vulnerability by sending an Electronic Key Segment with less than 0x18 bytes following the Key Format field. **CVE ID : CVE-2020-6085**		