National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures(CVE) Report

01 - 15 Apr 2020 Vol. 07 No. 07

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operating System					
3xlogic					
infinias_eidc32_firmware					
Improper Authentication	04-04-2020	7.5	3xLOGIC Infinias eIDC32 2.213 devices with Web 1.107 allow Authentication Bypass via CMD.HTM?CMD= because authentication depends on the client side's interpretation of the <KEY>MYKEY</KEY> substring. **CVE ID : CVE-2020-11542**	N/A	O-3XL-INFI-270420/1
infinias_eidc32_web					
Improper Authentication	04-04-2020	7.5	3xLOGIC Infinias eIDC32 2.213 devices with Web 1.107 allow Authentication Bypass via CMD.HTM?CMD= because authentication depends on the client side's interpretation of the <KEY>MYKEY</KEY> substring. **CVE ID : CVE-2020-11542**	N/A	O-3XL-INFI-270420/2
infinias_eidc32					
Improper Authentication	04-04-2020	7.5	3xLOGIC Infinias eIDC32 2.213 devices with Web 1.107 allow Authentication Bypass via CMD.HTM?CMD= because	N/A	O-3XL-INFI-270420/3

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authentication depends on the client side's interpretation of the <KEY>MYKEY</KEY> substring. **CVE ID : CVE-2020-11542**		
amcrest					
1080-lite_8ch_firmware					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	O-AMC-1080-270420/4
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**	N/A	O-AMC-1080-270420/5
amdv10814-h5_firmware					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	O-AMC-AMDV-270420/6

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
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**	N/A	O-AMC-AMDV-270420/7
ipm-721_firmware					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	O-AMC-IPM--270420/8
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**	N/A	O-AMC-IPM--270420/9
ip2m-841_firmware					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	O-AMC-IP2M-270420/10

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**	N/A	O-AMC-IP2M-270420/11
ip2m-841-v3_firmware					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	O-AMC-IP2M-270420/12
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**	N/A	O-AMC-IP2M-270420/13
ip2m-853ew_firmware					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	O-AMC-IP2M-270420/14

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**	N/A	O-AMC-IP2M-270420/15
ip2m-858w_firmware					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	O-AMC-IP2M-270420/16
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**	N/A	O-AMC-IP2M-270420/17
ip2m-866w_firmware					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	O-AMC-IP2M-270420/18

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**	N/A	O-AMC-IP2M-270420/19
ip2m-866ew_firmware					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	O-AMC-IP2M-270420/20
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**	N/A	O-AMC-IP2M-270420/21
ip4m-1053ew_firmware					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	O-AMC-IP4M-270420/22

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**	N/A	O-AMC-IP4M-270420/23
ip8m-2454ew_firmware					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	O-AMC-IP8M-270420/24
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**	N/A	O-AMC-IP8M-270420/25
ip8m-2493eb_firmware					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	O-AMC-IP8M-270420/26

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**	N/A	O-AMC-IP8M-270420/27
ip8m-2496eb_firmware					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	O-AMC-IP8M-270420/28
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**	N/A	O-AMC-IP8M-270420/29
ip8m-2597e_firmware					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	O-AMC-IP8M-270420/30

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
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**	N/A	O-AMC-IP8M-270420/31
ip8m-mb2546ew_firmware					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	O-AMC-IP8M-270420/32
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**	N/A	O-AMC-IP8M-270420/33
ip8m-mt2544ew_firmware					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	O-AMC-IP8M-270420/34

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**	N/A	O-AMC-IP8M-270420/35
ip8m-t2499ew_firmware					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	O-AMC-IP8M-270420/36
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**	N/A	O-AMC-IP8M-270420/37
ipm-hx1_firmware					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	O-AMC-IPM--270420/38

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**	N/A	O-AMC-IPM--270420/39
Apple					
mac_os					
Improper Certificate Validation	06-04-2020	6.4	An issue was discovered in Pulse Secure Pulse Connect Secure (PCS) through 2020-04-06. The applet in tncc.jar, executed on macOS, Linux, and Solaris clients when a Host Checker policy is enforced, accepts an arbitrary SSL certificate. **CVE ID : CVE-2020-11580**	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44426	O-APP-MAC_-270420/40
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-04-2020	9.3	An issue was discovered in Pulse Secure Pulse Connect Secure (PCS) through 2020-04-06. The applet in tncc.jar, executed on macOS, Linux, and Solaris clients when a Host Checker policy is enforced, allows a man-in-the-middle attacker to perform OS command injection attacks (against a client) via shell metacharacters to the doCustomRemediateInstr	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44426	O-APP-MAC_-270420/41

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
			uctions method, because Runtime.getRuntime().exec() is used. **CVE ID : CVE-2020-11581**		
Improper Restriction of Excessive Authentication Attempts	06-04-2020	3.3	An issue was discovered in Pulse Secure Pulse Connect Secure (PCS) through 2020-04-06. The applet in tncc.jar, executed on macOS, Linux, and Solaris clients when a Host Checker policy is enforced, launches a TCP server that accepts local connections on a random port. This can be reached by local HTTP clients, because up to 25 invalid lines are ignored, and because DNS rebinding can occur. (This server accepts, for example, a setcookie command that might be relevant to CVE-2020-11581 exploitation.) **CVE ID : CVE-2020-11582**	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44426	O-APP-MAC_-270420/42
iphone_os					
N/A	01-04-2020	6.8	This issue was addressed with improved checks. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. An application may be able to use arbitrary	N/A	O-APP-IPHO-270420/43

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			entitlements. **CVE ID : CVE-2020-3883**		
Always-Incorrect Control Flow Implementation	01-04-2020	4.3	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A file URL may be incorrectly processed. **CVE ID : CVE-2020-3885**	N/A	O-APP-IPHO-270420/44
N/A	01-04-2020	4.3	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A download's origin may be incorrectly associated. **CVE ID : CVE-2020-3887**	N/A	O-APP-IPHO-270420/45
N/A	01-04-2020	4.3	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4. A maliciously crafted page may interfere with other web contexts. **CVE ID : CVE-2020-3888**	N/A	O-APP-IPHO-270420/46
Exposure of Resource to Wrong Sphere	01-04-2020	5	The issue was addressed with improved deletion. This issue is fixed in iOS 13.4 and iPadOS 13.4.	N/A	O-APP-IPHO-270420/47

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Deleted messages groups may still be suggested as an autocompletion. **CVE ID : CVE-2020-3890**		
Missing Authorization	01-04-2020	2.1	A logic issue was addressed with improved state management. This issue is fixed in iOS 13.4 and iPadOS 13.4, watchOS 6.2. A person with physical access to a locked iOS device may be able to respond to messages even when replies are disabled. **CVE ID : CVE-2020-3891**	N/A	O-APP-IPHO-270420/48
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-04-2020	2.6	A race condition was addressed with additional validation. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. An application may be able to read restricted memory. **CVE ID : CVE-2020-3894**	N/A	O-APP-IPHO-270420/49
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-04-2020	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud	N/A	O-APP-IPHO-270420/50

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for Windows 7.18. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-3895**		
Access of Resource Using Incompatible Type ('Type Confusion')	01-04-2020	9.3	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2020-3897**	N/A	O-APP-IPHO-270420/51
Uncontrolled Resource Consumption	01-04-2020	9.3	A memory consumption issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2020-3899**	N/A	O-APP-IPHO-270420/52
Improper Restriction of Operations within the	01-04-2020	6.8	A memory corruption issue was addressed with improved memory handling. This issue is	N/A	O-APP-IPHO-270420/53

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-3900**		
Access of Resource Using Incompatible Type ('Type Confusion')	01-04-2020	6.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-3901**	N/A	O-APP-IPHO-270420/54
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-04-2020	4.3	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may	N/A	O-APP-IPHO-270420/55

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to a cross site scripting attack. **CVE ID : CVE-2020-3902**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-04-2020	7.5	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Multiple issues in libxml2. **CVE ID : CVE-2020-3909**	N/A	O-APP-IPHO-270420/56
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-04-2020	7.5	A buffer overflow was addressed with improved size validation. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Multiple issues in libxml2. **CVE ID : CVE-2020-3910**	N/A	O-APP-IPHO-270420/57
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-04-2020	7.5	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for	N/A	O-APP-IPHO-270420/58

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Windows 7.18. Multiple issues in libxml2. **CVE ID : CVE-2020-3911**		
Improper Privilege Management	01-04-2020	6.8	A permissions issue existed. This issue was addressed with improved permission validation. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, watchOS 6.2. A malicious application may be able to elevate privileges. **CVE ID : CVE-2020-3913**	N/A	O-APP-IPHO-270420/59
Improper Release of Memory Before Removing Last Reference	01-04-2020	4.3	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. An application may be able to read restricted memory. **CVE ID : CVE-2020-3914**	N/A	O-APP-IPHO-270420/60
Information Exposure	01-04-2020	5	An access issue was addressed with additional sandbox restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, watchOS 6.2. Setting an alternate app icon may disclose a photo without needing permission to access photos. **CVE ID : CVE-2020-3916**	N/A	O-APP-IPHO-270420/61
Exposure of Resource to	01-04-2020	2.1	This issue was addressed with a new entitlement. This issue is fixed in iOS	N/A	O-APP-IPHO-270420/62

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wrong Sphere			13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2. An application may be able to use an SSH client provided by private frameworks. **CVE ID : CVE-2020-3917**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-04-2020	9.3	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-3919**	N/A	O-APP-IPHO-270420/63
Use After Free	01-04-2020	9.3	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2020-9768**	N/A	O-APP-IPHO-270420/64
Inadequate Encryption Strength	01-04-2020	4	A logic issue was addressed with improved state management. This issue is fixed in iOS 13.4 and iPadOS 13.4. An attacker in a privileged network position may be able to intercept	N/A	O-APP-IPHO-270420/65

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Bluetooth traffic. **CVE ID : CVE-2020-9770**		
Information Exposure	01-04-2020	4.3	The issue was addressed with improved handling of icon caches. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. A malicious application may be able to identify what other applications a user has installed. **CVE ID : CVE-2020-9773**	N/A	O-APP-IPHO-270420/66
Improper Initialization	01-04-2020	5	An issue existed in the handling of tabs displaying picture in picture video. The issue was corrected with improved state handling. This issue is fixed in iOS 13.4 and iPadOS 13.4. A user's private browsing activity may be unexpectedly saved in Screen Time. **CVE ID : CVE-2020-9775**	N/A	O-APP-IPHO-270420/67
Improper Input Validation	01-04-2020	5	An issue existed in the selection of video file by Mail. The issue was fixed by selecting the latest version of a video. This issue is fixed in iOS 13.4 and iPadOS 13.4. Cropped videos may not be shared properly via Mail. **CVE ID : CVE-2020-9777**	N/A	O-APP-IPHO-270420/68
Information	01-04-2020	2.1	The issue was resolved by clearing application	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
Exposure			previews when content is deleted. This issue is fixed in iOS 13.4 and iPadOS 13.4. A local user may be able to view deleted content in the app switcher. **CVE ID : CVE-2020-9780**		270420/69
Improper Preservation of Permissions	01-04-2020	5	The issue was addressed by clearing website permission prompts after navigation. This issue is fixed in iOS 13.4 and iPadOS 13.4. A user may grant website permissions to a site they didn't intend to. **CVE ID : CVE-2020-9781**	N/A	O-APP-IPHO-270420/70
Use After Free	01-04-2020	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to code execution. **CVE ID : CVE-2020-9783**	N/A	O-APP-IPHO-270420/71
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-04-2020	9.3	Multiple memory corruption issues were addressed with improved state management. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS	N/A	O-APP-IPHO-270420/72

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			13.4, watchOS 6.2. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9785**		
mac_os_x					
Out-of-bounds Read	01-04-2020	10	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.3. A remote attacker may be able to leak memory. **CVE ID : CVE-2020-3847**	N/A	O-APP-MAC_-270420/73
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-04-2020	7.5	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.3. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-3848**	N/A	O-APP-MAC_-270420/74
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-04-2020	7.5	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.3. A remote attacker may be able to cause unexpected application termination or arbitrary code execution.	N/A	O-APP-MAC_-270420/75

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3849		
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-04-2020	7.5	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.3. A remote attacker may be able to cause unexpected application termination or arbitrary code execution. **CVE ID : CVE-2020-3850**	N/A	O-APP-MAC_-270420/76
Information Exposure	01-04-2020	2.1	A logic issue was addressed with improved state management. This issue is fixed in macOS Catalina 10.15.4. A local user may be able to view sensitive user information. **CVE ID : CVE-2020-3881**	N/A	O-APP-MAC_-270420/77
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	01-04-2020	4.3	An injection issue was addressed with improved validation. This issue is fixed in macOS Catalina 10.15.4. A remote attacker may be able to cause arbitrary javascript code execution. **CVE ID : CVE-2020-3884**	N/A	O-APP-MAC_-270420/78
Information Exposure	01-04-2020	2.1	A logic issue was addressed with improved state management. This issue is fixed in macOS Catalina 10.15.4. A local user may be able to read arbitrary files.	N/A	O-APP-MAC_-270420/79

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3889		
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-04-2020	9.3	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.4. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-3892**	N/A	O-APP-MAC_-270420/80
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-04-2020	9.3	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.4. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-3893**	N/A	O-APP-MAC_-270420/81
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-04-2020	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15.4. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2020-3903**	N/A	O-APP-MAC_-270420/82
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-04-2020	9.3	Multiple memory corruption issues were addressed with improved state management. This issue is fixed in macOS Catalina 10.15.4. A malicious application may be able to execute	N/A	O-APP-MAC_-270420/83

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with kernel privileges. **CVE ID : CVE-2020-3904**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-04-2020	9.3	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.4. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-3905**	N/A	O-APP-MAC_-270420/84
N/A	01-04-2020	6.8	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Catalina 10.15.4. A maliciously crafted application may be able to bypass code signing enforcement. **CVE ID : CVE-2020-3906**	N/A	O-APP-MAC_-270420/85
Out-of-bounds Read	01-04-2020	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-2020-3907**	N/A	O-APP-MAC_-270420/86
Out-of-bounds Read	01-04-2020	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	N/A	O-APP-MAC_-270420/87

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			be able to cause unexpected system termination or read kernel memory. **CVE ID : CVE-2020-3908**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-04-2020	7.5	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Multiple issues in libxml2. **CVE ID : CVE-2020-3909**	N/A	O-APP-MAC_-270420/88
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-04-2020	7.5	A buffer overflow was addressed with improved size validation. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Multiple issues in libxml2. **CVE ID : CVE-2020-3910**	N/A	O-APP-MAC_-270420/89
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-04-2020	7.5	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2, iTunes for Windows 12.10.5,	N/A	O-APP-MAC_-270420/90

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			iCloud for Windows 10.9.3, iCloud for Windows 7.18. Multiple issues in libxml2. **CVE ID : CVE-2020-3911**		
Out-of-bounds Read	01-04-2020	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-2020-3912**	N/A	O-APP-MAC_-270420/91
Improper Privilege Management	01-04-2020	6.8	A permissions issue existed. This issue was addressed with improved permission validation. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, watchOS 6.2. A malicious application may be able to elevate privileges. **CVE ID : CVE-2020-3913**	N/A	O-APP-MAC_-270420/92
Improper Release of Memory Before Removing Last Reference	01-04-2020	4.3	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. An application may be able to read restricted memory. **CVE ID : CVE-2020-3914**	N/A	O-APP-MAC_-270420/93

CVSS Scoring Scale	0-1	1-2	2-3	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	01-04-2020	9.3	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-3919**	N/A	O-APP-MAC_-270420/94
N/A	01-04-2020	7.5	Multiple issues were addressed by updating to version 8.1.1850. This issue is fixed in macOS Catalina 10.15.4. Multiple issues in Vim. **CVE ID : CVE-2020-9769**	N/A	O-APP-MAC_-270420/95
Information Exposure	01-04-2020	4.3	The issue was addressed with improved handling of icon caches. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. A malicious application may be able to identify what other applications a user has installed. **CVE ID : CVE-2020-9773**	N/A	O-APP-MAC_-270420/96
Information Exposure	01-04-2020	4.3	This issue was addressed with a new entitlement. This issue is fixed in macOS Catalina 10.15.4. A malicious application may be able to access a user's call history.	N/A	O-APP-MAC_-270420/97

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9776		
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-04-2020	9.3	Multiple memory corruption issues were addressed with improved state management. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9785**	N/A	O-APP-MAC_-270420/98
watchos					
N/A	01-04-2020	6.8	This issue was addressed with improved checks. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. An application may be able to use arbitrary entitlements. **CVE ID : CVE-2020-3883**	N/A	O-APP-WATC-270420/99
Missing Authorization	01-04-2020	2.1	A logic issue was addressed with improved state management. This issue is fixed in iOS 13.4 and iPadOS 13.4, watchOS 6.2. A person with physical access to a locked iOS device may be able to respond to messages even when replies are disabled. **CVE ID : CVE-2020-3891**	N/A	O-APP-WATC-270420/100
Improper Restriction of	01-04-2020	9.3	A memory corruption issue was addressed with	N/A	O-APP-WATC-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-3895**		270420/101
Access of Resource Using Incompatible Type ('Type Confusion')	01-04-2020	9.3	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2020-3897**	N/A	O-APP-WATC-270420/102
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-04-2020	6.8	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18.	N/A	O-APP-WATC-270420/103

CVSS Scoring Scale	0-1	1-2	2-3	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-2020-3900**		
Access of Resource Using Incompatible Type ('Type Confusion')	01-04-2020	6.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-3901**	N/A	O-APP-WATC-270420/104
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-04-2020	7.5	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Multiple issues in libxml2. **CVE ID : CVE-2020-3909**	N/A	O-APP-WATC-270420/105
Buffer Copy without Checking Size of Input ('Classic Buffer	01-04-2020	7.5	A buffer overflow was addressed with improved size validation. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS	N/A	O-APP-WATC-270420/106

CVSS Scoring Scale	0-1	1-2	2-3	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')			Catalina 10.15.4, tvOS 13.4, watchOS 6.2, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Multiple issues in libxml2. **CVE ID : CVE-2020-3910**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-04-2020	7.5	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Multiple issues in libxml2. **CVE ID : CVE-2020-3911**	N/A	O-APP-WATC-270420/107
Improper Privilege Management	01-04-2020	6.8	A permissions issue existed. This issue was addressed with improved permission validation. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, watchOS 6.2. A malicious application may be able to elevate privileges. **CVE ID : CVE-2020-3913**	N/A	O-APP-WATC-270420/108
Improper Release of Memory Before Removing Last Reference	01-04-2020	4.3	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS	N/A	O-APP-WATC-270420/109

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			13.4, watchOS 6.2. An application may be able to read restricted memory. **CVE ID : CVE-2020-3914**		
Information Exposure	01-04-2020	5	An access issue was addressed with additional sandbox restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, watchOS 6.2. Setting an alternate app icon may disclose a photo without needing permission to access photos. **CVE ID : CVE-2020-3916**	N/A	O-APP-WATC-270420/110
Exposure of Resource to Wrong Sphere	01-04-2020	2.1	This issue was addressed with a new entitlement. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2. An application may be able to use an SSH client provided by private frameworks. **CVE ID : CVE-2020-3917**	N/A	O-APP-WATC-270420/111
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-04-2020	9.3	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-3919**	N/A	O-APP-WATC-270420/112

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
Use After Free	01-04-2020	9.3	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2020-9768**	N/A	O-APP-WATC-270420/113
Information Exposure	01-04-2020	4.3	The issue was addressed with improved handling of icon caches. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. A malicious application may be able to identify what other applications a user has installed. **CVE ID : CVE-2020-9773**	N/A	O-APP-WATC-270420/114
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-04-2020	9.3	Multiple memory corruption issues were addressed with improved state management. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9785**	N/A	O-APP-WATC-270420/115
tvos					
N/A	01-04-2020	6.8	This issue was addressed with improved checks.	N/A	O-APP-TVOS-270420/116

CVSS Scoring Scale	0-1	1-2	2-3	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 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. An application may be able to use arbitrary entitlements. **CVE ID : CVE-2020-3883**		
Always-Incorrect Control Flow Implementation	01-04-2020	4.3	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A file URL may be incorrectly processed. **CVE ID : CVE-2020-3885**	N/A	O-APP-TVOS-270420/117
N/A	01-04-2020	4.3	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A download's origin may be incorrectly associated. **CVE ID : CVE-2020-3887**	N/A	O-APP-TVOS-270420/118
Concurrent Execution using Shared Resource with Improper Synchronization ('Race	01-04-2020	2.6	A race condition was addressed with additional validation. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud	N/A	O-APP-TVOS-270420/119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Condition')			for Windows 10.9.3, iCloud for Windows 7.18. An application may be able to read restricted memory. **CVE ID : CVE-2020-3894**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-04-2020	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-3895**	N/A	O-APP-TVOS-270420/120
Access of Resource Using Incompatible Type ('Type Confusion')	01-04-2020	9.3	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2020-3897**	N/A	O-APP-TVOS-270420/121
Uncontrolled Resource	01-04-2020	9.3	A memory consumption issue was addressed with	N/A	O-APP-TVOS-270420/122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Consumption			improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2020-3899**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-04-2020	6.8	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-3900**	N/A	O-APP-TVOS-270420/123
Access of Resource Using Incompatible Type ('Type Confusion')	01-04-2020	6.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously	N/A	O-APP-TVOS-270420/124

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-3901**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-04-2020	4.3	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to a cross site scripting attack. **CVE ID : CVE-2020-3902**	N/A	O-APP-TVOS-270420/125
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-04-2020	7.5	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Multiple issues in libxml2. **CVE ID : CVE-2020-3909**	N/A	O-APP-TVOS-270420/126
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-04-2020	7.5	A buffer overflow was addressed with improved size validation. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2, iTunes	N/A	O-APP-TVOS-270420/127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Multiple issues in libxml2. **CVE ID : CVE-2020-3910**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-04-2020	7.5	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Multiple issues in libxml2. **CVE ID : CVE-2020-3911**	N/A	O-APP-TVOS-270420/128
Improper Release of Memory Before Removing Last Reference	01-04-2020	4.3	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. An application may be able to read restricted memory. **CVE ID : CVE-2020-3914**	N/A	O-APP-TVOS-270420/129
Exposure of Resource to Wrong Sphere	01-04-2020	2.1	This issue was addressed with a new entitlement. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2. An application may be able to use an SSH client provided by private frameworks.	N/A	O-APP-TVOS-270420/130

CVSS Scoring Scale	0-1	1-2	2-3	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-2020-3917		
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-04-2020	9.3	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-3919**	N/A	O-APP-TVOS-270420/131
Use After Free	01-04-2020	9.3	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2020-9768**	N/A	O-APP-TVOS-270420/132
Information Exposure	01-04-2020	4.3	The issue was addressed with improved handling of icon caches. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. A malicious application may be able to identify what other applications a user has installed. **CVE ID : CVE-2020-9773**	N/A	O-APP-TVOS-270420/133
Use After Free	01-04-2020	6.8	A use after free issue was addressed with improved	N/A	O-APP-TVOS-270420/134

CVSS Scoring Scale	0-1	1-2	2-3	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 management. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to code execution. **CVE ID : CVE-2020-9783**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-04-2020	9.3	Multiple memory corruption issues were addressed with improved state management. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9785**	N/A	O-APP-TVOS-270420/135
ipados					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-04-2020	7.5	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Multiple issues in libxml2. **CVE ID : CVE-2020-3909**	N/A	O-APP-IPAD-270420/136

CVSS Scoring Scale	0-1	1-2	2-3	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')	01-04-2020	7.5	A buffer overflow was addressed with improved size validation. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Multiple issues in libxml2. **CVE ID : CVE-2020-3910**	N/A	O-APP-IPAD-270420/137
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-04-2020	7.5	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Multiple issues in libxml2. **CVE ID : CVE-2020-3911**	N/A	O-APP-IPAD-270420/138
Improper Privilege Management	01-04-2020	6.8	A permissions issue existed. This issue was addressed with improved permission validation. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, watchOS 6.2. A malicious application may be able to elevate privileges. **CVE ID : CVE-2020-3913**	N/A	O-APP-IPAD-270420/139
Improper Release of	01-04-2020	4.3	A memory initialization issue was addressed with	N/A	O-APP-IPAD-270420/140

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Before Removing Last Reference			improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. An application may be able to read restricted memory. **CVE ID : CVE-2020-3914**		
Information Exposure	01-04-2020	5	An access issue was addressed with additional sandbox restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, watchOS 6.2. Setting an alternate app icon may disclose a photo without needing permission to access photos. **CVE ID : CVE-2020-3916**	N/A	O-APP-IPAD-270420/141
Exposure of Resource to Wrong Sphere	01-04-2020	2.1	This issue was addressed with a new entitlement. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2. An application may be able to use an SSH client provided by private frameworks. **CVE ID : CVE-2020-3917**	N/A	O-APP-IPAD-270420/142
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-04-2020	9.3	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. A malicious application may	N/A	O-APP-IPAD-270420/143

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-3919**		
Use After Free	01-04-2020	9.3	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2. An application may be able to execute arbitrary code with system privileges. **CVE ID : CVE-2020-9768**	N/A	O-APP-IPAD-270420/144
Inadequate Encryption Strength	01-04-2020	4	A logic issue was addressed with improved state management. This issue is fixed in iOS 13.4 and iPadOS 13.4. An attacker in a privileged network position may be able to intercept Bluetooth traffic. **CVE ID : CVE-2020-9770**	N/A	O-APP-IPAD-270420/145
Information Exposure	01-04-2020	4.3	The issue was addressed with improved handling of icon caches. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. A malicious application may be able to identify what other applications a user has installed. **CVE ID : CVE-2020-9773**	N/A	O-APP-IPAD-270420/146
Improper	01-04-2020	5	An issue existed in the handling of tabs	N/A	O-APP-IPAD-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Initialization			displaying picture in picture video. The issue was corrected with improved state handling. This issue is fixed in iOS 13.4 and iPadOS 13.4. A user's private browsing activity may be unexpectedly saved in Screen Time. **CVE ID : CVE-2020-9775**		270420/147
Improper Input Validation	01-04-2020	5	An issue existed in the selection of video file by Mail. The issue was fixed by selecting the latest version of a video. This issue is fixed in iOS 13.4 and iPadOS 13.4. Cropped videos may not be shared properly via Mail. **CVE ID : CVE-2020-9777**	N/A	O-APP-IPAD-270420/148
Information Exposure	01-04-2020	2.1	The issue was resolved by clearing application previews when content is deleted. This issue is fixed in iOS 13.4 and iPadOS 13.4. A local user may be able to view deleted content in the app switcher. **CVE ID : CVE-2020-9780**	N/A	O-APP-IPAD-270420/149
Improper Preservation of Permissions	01-04-2020	5	The issue was addressed by clearing website permission prompts after navigation. This issue is fixed in iOS 13.4 and iPadOS 13.4. A user may grant website permissions to a site they	N/A	O-APP-IPAD-270420/150

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			didn't intend to. **CVE ID : CVE-2020-9781**		
Use After Free	01-04-2020	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to code execution. **CVE ID : CVE-2020-9783**	N/A	O-APP-IPAD-270420/151
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-04-2020	9.3	Multiple memory corruption issues were addressed with improved state management. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. A malicious application may be able to execute arbitrary code with kernel privileges. **CVE ID : CVE-2020-9785**	N/A	O-APP-IPAD-270420/152
ipad_os					
N/A	01-04-2020	6.8	This issue was addressed with improved checks. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. An application may be able to use arbitrary entitlements.	N/A	O-APP-IPAD-270420/153

CVSS Scoring Scale	0-1	1-2	2-3	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-2020-3883		
Always-Incorrect Control Flow Implementation	01-04-2020	4.3	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A file URL may be incorrectly processed. **CVE ID : CVE-2020-3885**	N/A	O-APP-IPAD-270420/154
N/A	01-04-2020	4.3	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A download's origin may be incorrectly associated. **CVE ID : CVE-2020-3887**	N/A	O-APP-IPAD-270420/155
N/A	01-04-2020	4.3	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4. A maliciously crafted page may interfere with other web contexts. **CVE ID : CVE-2020-3888**	N/A	O-APP-IPAD-270420/156
Exposure of Resource to Wrong Sphere	01-04-2020	5	The issue was addressed with improved deletion. This issue is fixed in iOS 13.4 and iPadOS 13.4. Deleted messages groups	N/A	O-APP-IPAD-270420/157

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
			may still be suggested as an autocompletion. **CVE ID : CVE-2020-3890**		
Missing Authorization	01-04-2020	2.1	A logic issue was addressed with improved state management. This issue is fixed in iOS 13.4 and iPadOS 13.4, watchOS 6.2. A person with physical access to a locked iOS device may be able to respond to messages even when replies are disabled. **CVE ID : CVE-2020-3891**	N/A	O-APP-IPAD-270420/158
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-04-2020	2.6	A race condition was addressed with additional validation. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. An application may be able to read restricted memory. **CVE ID : CVE-2020-3894**	N/A	O-APP-IPAD-270420/159
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-04-2020	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18.	N/A	O-APP-IPAD-270420/160

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-3895**		
Access of Resource Using Incompatible Type ('Type Confusion')	01-04-2020	9.3	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2020-3897**	N/A	O-APP-IPAD-270420/161
Uncontrolled Resource Consumption	01-04-2020	9.3	A memory consumption issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2020-3899**	N/A	O-APP-IPAD-270420/162
Improper Restriction of Operations within the Bounds of a	01-04-2020	6.8	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and	N/A	O-APP-IPAD-270420/163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-3900**		
Access of Resource Using Incompatible Type ('Type Confusion')	01-04-2020	6.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-3901**	N/A	O-APP-IPAD-270420/164
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-04-2020	4.3	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to a cross site	N/A	O-APP-IPAD-270420/165

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			scripting attack. **CVE ID : CVE-2020-3902**		
BD					
pyxis_medstation_es_firmware					
Information Exposure	01-04-2020	3.6	In BD Pyxis MedStation ES System v1.6.1 and Pyxis Anesthesia (PAS) ES System v1.6.1, a restricted desktop environment escape vulnerability exists in the kiosk mode functionality of affected devices. Specially crafted inputs could allow the user to escape the restricted environment, resulting in access to sensitive data. **CVE ID : CVE-2020-10598**	N/A	O-BD-PYXI-270420/166
pyxis_anesthesia_station_es_firmware					
Information Exposure	01-04-2020	3.6	In BD Pyxis MedStation ES System v1.6.1 and Pyxis Anesthesia (PAS) ES System v1.6.1, a restricted desktop environment escape vulnerability exists in the kiosk mode functionality of affected devices. Specially crafted inputs could allow the user to escape the restricted environment, resulting in access to sensitive data. **CVE ID : CVE-2020-10598**	N/A	O-BD-PYXI-270420/167
cacagoo					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
tv-288zd-2mp_firmware					
Improper Authentication	02-04-2020	10	CACAGOO Cloud Storage Intelligent Camera TV-288ZD-2MP with firmware 3.4.2.0919 has weak authentication of TELNET access, leading to root privileges without any password required. **CVE ID : CVE-2020-6852**	N/A	O-CAC-TV-2-270420/168
Missing Authorization	02-04-2020	5	The CACAGOO Cloud Storage Intelligent Camera TV-288ZD-2MP with firmware 3.4.2.0919 allows access to the RTSP service without a password. **CVE ID : CVE-2020-9349**	N/A	O-CAC-TV-2-270420/169
Canonical					
ubuntu_linux					
Information Exposure	10-04-2020	2.1	The fix for the Linux kernel in Ubuntu 18.04 LTS for CVE-2019-14615 ("The Linux kernel did not properly clear data structures on context switches for certain Intel graphics processors.") was discovered to be incomplete, meaning that in versions of the kernel before 4.15.0-91.92, an attacker could use this vulnerability to expose sensitive information. **CVE ID : CVE-2020-8832**	N/A	O-CAN-UBUN-270420/170
Improper Restriction of	02-04-2020	7.2	In the Linux kernel 5.5.0 and newer, the bpf	https://git.kernel.org/	O-CAN-UBUN-270420/171

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
Operations within the Bounds of a Memory Buffer			verifier (kernel/bpf/verifier.c) did not properly restrict the register bounds for 32-bit operations, leading to out-of-bounds reads and writes in kernel memory. The vulnerability also affects the Linux 5.4 stable series, starting with v5.4.7, as the introducing commit was backported to that branch. This vulnerability was fixed in 5.6.1, 5.5.14, and 5.4.29. (issue is aka ZDI-CAN-10780) **CVE ID : CVE-2020-8835**	pub/scm/linux/kernel/git/netdev/net-next.git/commit/?id=f2d67fec0b43edce8c416101cdc52e71145b5fef, https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=f2d67fec0b43edce8c416101cdc52e71145b5fef	
dahua					
sd6al_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go down. **CVE ID : CVE-2020-9499**	N/A	O-DAH-SD6A-270420/172
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query	N/A	O-DAH-SD6A-270420/173

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			command, which may cause the device to go down. **CVE ID : CVE-2020-9500**		
sd5a_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go down. **CVE ID : CVE-2020-9499**	N/A	O-DAH-SD5A-270420/174
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go down. **CVE ID : CVE-2020-9500**	N/A	O-DAH-SD5A-270420/175
sd1a_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go down. **CVE ID : CVE-2020-9499**	N/A	O-DAH-SD1A-270420/176
Improper Input	09-04-2020	5	Some products of Dahua have Denial of Service	N/A	O-DAH-SD1A-270420/177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go down. **CVE ID : CVE-2020-9500**		
ptz1a_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go down. **CVE ID : CVE-2020-9499**	N/A	O-DAH-PTZ1-270420/178
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go down. **CVE ID : CVE-2020-9500**	N/A	O-DAH-PTZ1-270420/179
sd50_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go	N/A	O-DAH-SD50-270420/180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			down. **CVE ID : CVE-2020-9499**		
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go down. **CVE ID : CVE-2020-9500**	N/A	O-DAH-SD50-270420/181
sd52c_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go down. **CVE ID : CVE-2020-9499**	N/A	O-DAH-SD52-270420/182
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go down. **CVE ID : CVE-2020-9500**	N/A	O-DAH-SD52-270420/183
ipc-hx5842h_firmware					
Buffer Copy without Checking Size of Input	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the	N/A	O-DAH-IPC--270420/184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			legal account, the attacker sends a specific DDNS test command, which may cause the device to go down. **CVE ID : CVE-2020-9499**		
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go down. **CVE ID : CVE-2020-9500**	N/A	O-DAH-IPC--270420/185
ipc-hx7842h_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go down. **CVE ID : CVE-2020-9499**	N/A	O-DAH-IPC--270420/186
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go down. **CVE ID : CVE-2020-9500**	N/A	O-DAH-IPC--270420/187
ipc-hx2xxx_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go down. **CVE ID : CVE-2020-9499**	N/A	O-DAH-IPC--270420/188
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go down. **CVE ID : CVE-2020-9500**	N/A	O-DAH-IPC--270420/189
ipc-hxxx5x4x_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go down. **CVE ID : CVE-2020-9499**	N/A	O-DAH-IPC--270420/190
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go	N/A	O-DAH-IPC--270420/191

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			down. **CVE ID : CVE-2020-9500**		
n42b1p_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go down. **CVE ID : CVE-2020-9499**	N/A	O-DAH-N42B-270420/192
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go down. **CVE ID : CVE-2020-9500**	N/A	O-DAH-N42B-270420/193
n42b2p_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go down. **CVE ID : CVE-2020-9499**	N/A	O-DAH-N42B-270420/194
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the	N/A	O-DAH-N42B-270420/195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			legal account, the attacker sends a specific log query command, which may cause the device to go down. **CVE ID : CVE-2020-9500**		
n42b3p_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go down. **CVE ID : CVE-2020-9499**	N/A	O-DAH-N42B-270420/196
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go down. **CVE ID : CVE-2020-9500**	N/A	O-DAH-N42B-270420/197
n52a4p_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go down. **CVE ID : CVE-2020-9499**	N/A	O-DAH-N52A-270420/198

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go down. **CVE ID : CVE-2020-9500**	N/A	O-DAH-N52A-270420/199
n54a4p_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go down. **CVE ID : CVE-2020-9499**	N/A	O-DAH-N54A-270420/200
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go down. **CVE ID : CVE-2020-9500**	N/A	O-DAH-N54A-270420/201
n52b2p_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may	N/A	O-DAH-N52B-270420/202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cause the device to go down. **CVE ID : CVE-2020-9499**		
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go down. **CVE ID : CVE-2020-9500**	N/A	O-DAH-N52B-270420/203
n52b5p_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go down. **CVE ID : CVE-2020-9499**	N/A	O-DAH-N52B-270420/204
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go down. **CVE ID : CVE-2020-9500**	N/A	O-DAH-N52B-270420/205
n52b3p_firmware					
Buffer Copy without Checking Size	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the	N/A	O-DAH-N52B-270420/206

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go down. **CVE ID : CVE-2020-9499**		
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go down. **CVE ID : CVE-2020-9500**	N/A	O-DAH-N52B-270420/207
n54b2p_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go down. **CVE ID : CVE-2020-9499**	N/A	O-DAH-N54B-270420/208
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go down. **CVE ID : CVE-2020-9500**	N/A	O-DAH-N54B-270420/209

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Debian					
debian_linux					
Out-of-bounds Write	02-04-2020	6.5	In hpack_dht_insert in hpack-tbl.c in the HPACK decoder in HAProxy 1.8 through 2.x before 2.1.4, a remote attacker can write arbitrary bytes around a certain location on the heap via a crafted HTTP/2 request, possibly causing remote code execution. **CVE ID : CVE-2020-11100**	https://bugzilla.redhat.com/show_bug.cgi?id=1819111, https://bugzilla.suse.com/show_bug.cgi?id=1168023, https://git.haproxy.org/?p=haproxy.git;a=commit;h=5dfc5d5cd0d2128d77253ead3acf03a421ab5b88, https://www.haproxy.org/download/2.1/src/CHANGELOG	O-DEB-DEBI-270420/210
Use of a Broken or Risky Cryptographic Algorithm	03-04-2020	6.4	GnuTLS 3.6.x before 3.6.13 uses incorrect cryptography for DTLS. The earliest affected version is 3.6.3 (2018-07-16) because of an error in a 2017-10-06 commit. The DTLS client always uses 32 '\0' bytes instead of a random value, and thus contributes no randomness to a DTLS negotiation. This breaks the security guarantees of	N/A	O-DEB-DEBI-270420/211

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the DTLS protocol. **CVE ID : CVE-2020-11501**		
Dell					
latitude_7202_firmware					
Use After Free	04-04-2020	7.2	Dell Latitude 7202 Rugged Tablet BIOS versions prior to A28 contain a UAF vulnerability in EFI_BOOT_SERVICES in system management mode. A local unauthenticated attacker may exploit this vulnerability by overwriting the EFI_BOOT_SERVICES structure to execute arbitrary code in system management mode. **CVE ID : CVE-2020-5348**	N/A	O-DEL-LATI-270420/212
r1-2210_firmware					
Information Exposure	10-04-2020	5	Dell EMC Networking X-Series firmware versions 3.0.1.2 and older, Dell EMC Networking PC5500 firmware versions 4.1.0.22 and older and Dell EMC PowerEdge VRTX Switch Modules firmware versions 2.0.0.77 and older contain an information disclosure vulnerability. A remote unauthenticated attacker could exploit this vulnerability to retrieve sensitive data by sending	N/A	O-DEL-R1-2-270420/213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a specially crafted request to the affected endpoints. **CVE ID : CVE-2020-5330**		
r1-2401_firmware					
Information Exposure	10-04-2020	5	Dell EMC Networking X-Series firmware versions 3.0.1.2 and older, Dell EMC Networking PC5500 firmware versions 4.1.0.22 and older and Dell EMC PowerEdge VRTX Switch Modules firmware versions 2.0.0.77 and older contain an information disclosure vulnerability. A remote unauthenticated attacker could exploit this vulnerability to retrieve sensitive data by sending a specially crafted request to the affected endpoints. **CVE ID : CVE-2020-5330**	N/A	O-DEL-R1-2-270420/214
pc5500_firmware					
Information Exposure	10-04-2020	5	Dell EMC Networking X-Series firmware versions 3.0.1.2 and older, Dell EMC Networking PC5500 firmware versions 4.1.0.22 and older and Dell EMC PowerEdge VRTX Switch Modules firmware versions 2.0.0.77 and older contain an information disclosure vulnerability. A remote unauthenticated attacker could exploit this vulnerability to retrieve	N/A	O-DEL-PC55-270420/215

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sensitive data by sending a specially crafted request to the affected endpoints. **CVE ID : CVE-2020-5330**		
x1000_firmware					
Information Exposure	10-04-2020	5	Dell EMC Networking X-Series firmware versions 3.0.1.2 and older, Dell EMC Networking PC5500 firmware versions 4.1.0.22 and older and Dell EMC PowerEdge VRTX Switch Modules firmware versions 2.0.0.77 and older contain an information disclosure vulnerability. A remote unauthenticated attacker could exploit this vulnerability to retrieve sensitive data by sending a specially crafted request to the affected endpoints. **CVE ID : CVE-2020-5330**	N/A	O-DEL-X100-270420/216
x4012_firmware					
Information Exposure	10-04-2020	5	Dell EMC Networking X-Series firmware versions 3.0.1.2 and older, Dell EMC Networking PC5500 firmware versions 4.1.0.22 and older and Dell EMC PowerEdge VRTX Switch Modules firmware versions 2.0.0.77 and older contain an information disclosure vulnerability. A remote unauthenticated attacker could exploit this	N/A	O-DEL-X401-270420/217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to retrieve sensitive data by sending a specially crafted request to the affected endpoints. **CVE ID : CVE-2020-5330**		
Dlink					
dsl-gs225_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	10-04-2020	6.5	D-Link DSL-GS225 J1 AU_1.0.4 devices allow an admin to execute OS commands by placing shell metacharacters after a supported CLI command, as demonstrated by ping -c1 127.0.0.1; cat/etc/passwd. The CLI is reachable by TELNET. **CVE ID : CVE-2020-6765**	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10165	O-DLI-DSL--270420/218
etentech					
psg-6528vm_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-04-2020	3.5	eten PSG-6528VM 1.1 devices allow XSS via System Contact or System Location. **CVE ID : CVE-2020-11714**	N/A	O-ETE-PSG--270420/219
Fedoraproject					
fedora					
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-04-2020	7.2	In the Linux kernel 5.5.0 and newer, the bpf verifier (kernel/bpf/verifier.c) did not properly restrict the register bounds for 32-bit operations, leading to out-of-bounds reads	https://git.kernel.org/pub/scm/linux/kernel/git/netdev/net-next.git/commit/?id=f	O-FED-FEDO-270420/220

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and writes in kernel memory. The vulnerability also affects the Linux 5.4 stable series, starting with v5.4.7, as the introducing commit was backported to that branch. This vulnerability was fixed in 5.6.1, 5.5.14, and 5.4.29. (issue is aka ZDI-CAN-10780) **CVE ID : CVE-2020-8835**	2d67fec0b43edce8c416101cdc52e71145b5fef, https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=f2d67fec0b43edce8c416101cdc52e71145b5fef	
Fortinet					
fortiadc_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-04-2020	3.5	An improper neutralization of input vulnerability in the dashboard of FortiADC may allow an authenticated attacker to perform a cross site scripting attack (XSS) via the name parameter. **CVE ID : CVE-2020-6647**	N/A	O-FOR-FORT-270420/221
Incorrect Authorization	07-04-2020	6.8	An improper authorization vulnerability in FortiADC may allow a remote authenticated user with low privileges to perform certain actions such as rebooting the system. **CVE ID : CVE-2020-9286**	N/A	O-FOR-FORT-270420/222
Google					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
android					
Out-of-bounds Write	08-04-2020	10	An issue was discovered on Samsung mobile devices with Q(10.0) software. There is arbitrary code execution in the Fingerprint Trustlet via a memory overwrite. The Samsung IDs are SVE-2019-16587, SVE-2019-16588, SVE-2019-16589 (April 2020). **CVE ID : CVE-2020-11600**	http://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-270420/223
Missing Authorization	08-04-2020	2.1	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) software. There is unauthorized access to applications in the Secure Folder via floating icons. The Samsung ID is SVE-2019-16195 (April 2020). **CVE ID : CVE-2020-11601**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-270420/224
Information Exposure	08-04-2020	2.1	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) software. Google Assistant leaks clipboard contents on a locked device. The Samsung ID is SVE-2019-16558 (April 2020). **CVE ID : CVE-2020-11602**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-270420/225
Access of Resource Using Incompatible	08-04-2020	7.5	An issue was discovered on Samsung mobile devices with P(9.0) and	https://security.samsungmobile.co	O-GOO-ANDR-270420/226

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Type ('Type Confusion')			Q(10.0) (incorporating TEEGRIS) software. Type confusion in the MLDAP Trustlet allows arbitrary code execution. The Samsung ID is SVE-2020-16599 (April 2020). **CVE ID : CVE-2020-11603**	m/securityUpdate.smsb	
Out-of-bounds Read	08-04-2020	6.4	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) (incorporating TEEGRIS) software. There is an Out-of-bounds read in the MLDAP Trustlet. The Samsung ID is SVE-2019-16565 (April 2020). **CVE ID : CVE-2020-11604**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-270420/227
Information Exposure	08-04-2020	5	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. There is sensitive information exposure from dumpstate in NFC logs. The Samsung ID is SVE-2019-16359 (April 2020). **CVE ID : CVE-2020-11605**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-270420/228
Information Exposure	08-04-2020	2.1	An issue was discovered on Samsung mobile devices with Q(10.0) software. Information about application preview (in the Secure Folder) leaks on a locked device.	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-270420/229

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
			The Samsung ID is SVE-2019-16463 (April 2020). **CVE ID : CVE-2020-11606**		
Information Exposure	08-04-2020	5	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) software. Notification exposure occurs in Lockdown mode because of the Edge Lighting application. The Samsung ID is SVE-2020-16680 (April 2020). **CVE ID : CVE-2020-11607**	https://security.samsungmobile.com/securityUpdate.smsb	O-GOO-ANDR-270420/230
Grandstream					
gxp1610_firmware					
Improper Link Resolution Before File Access ('Link Following')	14-04-2020	9	Grandstream GXP1600 series firmware 1.0.4.152 and below is vulnerable to authenticated remote command execution when an attacker uploads a specially crafted tar file to the HTTP /cgi-bin/upload_vpntar interface. **CVE ID : CVE-2020-5738**	N/A	O-GRA-GXP1-270420/231
Improper Control of Generation of Code ('Code Injection')	14-04-2020	9	Grandstream GXP1600 series firmware 1.0.4.152 and below is vulnerable to authenticated remote command execution when an attacker adds an OpenVPN up script to the phone's VPN settings via the "Additional Settings" field in the web interface.	N/A	O-GRA-GXP1-270420/232

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			When the VPN's connection is established, the user defined script is executed with root privileges. **CVE ID : CVE-2020-5739**		
gxp1615_firmware					
Improper Link Resolution Before File Access ('Link Following')	14-04-2020	9	Grandstream GXP1600 series firmware 1.0.4.152 and below is vulnerable to authenticated remote command execution when an attacker uploads a specially crafted tar file to the HTTP /cgi-bin/upload_vpntar interface. **CVE ID : CVE-2020-5738**	N/A	O-GRA-GXP1-270420/233
Improper Control of Generation of Code ('Code Injection')	14-04-2020	9	Grandstream GXP1600 series firmware 1.0.4.152 and below is vulnerable to authenticated remote command execution when an attacker adds an OpenVPN up script to the phone's VPN settings via the "Additional Settings" field in the web interface. When the VPN's connection is established, the user defined script is executed with root privileges. **CVE ID : CVE-2020-5739**	N/A	O-GRA-GXP1-270420/234
gxp1620_firmware					
Improper Link Resolution Before File Access ('Link	14-04-2020	9	Grandstream GXP1600 series firmware 1.0.4.152 and below is vulnerable to authenticated remote	N/A	O-GRA-GXP1-270420/235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Following')			command execution when an attacker uploads a specially crafted tar file to the HTTP /cgi-bin/upload_vpntar interface. **CVE ID : CVE-2020-5738**		
Improper Control of Generation of Code ('Code Injection')	14-04-2020	9	Grandstream GXP1600 series firmware 1.0.4.152 and below is vulnerable to authenticated remote command execution when an attacker adds an OpenVPN up script to the phone's VPN settings via the "Additional Settings" field in the web interface. When the VPN's connection is established, the user defined script is executed with root privileges. **CVE ID : CVE-2020-5739**	N/A	O-GRA-GXP1-270420/236
gxp1625_firmware					
Improper Link Resolution Before File Access ('Link Following')	14-04-2020	9	Grandstream GXP1600 series firmware 1.0.4.152 and below is vulnerable to authenticated remote command execution when an attacker uploads a specially crafted tar file to the HTTP /cgi-bin/upload_vpntar interface. **CVE ID : CVE-2020-5738**	N/A	O-GRA-GXP1-270420/237
Improper Control of Generation of Code ('Code	14-04-2020	9	Grandstream GXP1600 series firmware 1.0.4.152 and below is vulnerable to authenticated remote	N/A	O-GRA-GXP1-270420/238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			command execution when an attacker adds an OpenVPN up script to the phone's VPN settings via the "Additional Settings" field in the web interface. When the VPN's connection is established, the user defined script is executed with root privileges. **CVE ID : CVE-2020-5739**		
gxp1628_firmware					
Improper Link Resolution Before File Access ('Link Following')	14-04-2020	9	Grandstream GXP1600 series firmware 1.0.4.152 and below is vulnerable to authenticated remote command execution when an attacker uploads a specially crafted tar file to the HTTP /cgi-bin/upload_vpntar interface. **CVE ID : CVE-2020-5738**	N/A	O-GRA-GXP1-270420/239
Improper Control of Generation of Code ('Code Injection')	14-04-2020	9	Grandstream GXP1600 series firmware 1.0.4.152 and below is vulnerable to authenticated remote command execution when an attacker adds an OpenVPN up script to the phone's VPN settings via the "Additional Settings" field in the web interface. When the VPN's connection is established, the user defined script is executed with root privileges.	N/A	O-GRA-GXP1-270420/240

CVSS Scoring Scale	0-1	1-2	2-3	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-2020-5739		
gxp1630_firmware					
Improper Link Resolution Before File Access ('Link Following')	14-04-2020	9	Grandstream GXP1600 series firmware 1.0.4.152 and below is vulnerable to authenticated remote command execution when an attacker uploads a specially crafted tar file to the HTTP /cgi-bin/upload_vpntar interface. **CVE ID : CVE-2020-5738**	N/A	O-GRA-GXP1-270420/241
Improper Control of Generation of Code ('Code Injection')	14-04-2020	9	Grandstream GXP1600 series firmware 1.0.4.152 and below is vulnerable to authenticated remote command execution when an attacker adds an OpenVPN up script to the phone's VPN settings via the "Additional Settings" field in the web interface. When the VPN's connection is established, the user defined script is executed with root privileges. **CVE ID : CVE-2020-5739**	N/A	O-GRA-GXP1-270420/242
hirschmann					
hios					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-04-2020	7.5	A buffer overflow vulnerability was found in some devices of Hirschmann Automation and Control HiOS and HiSecOS. The vulnerability is due to improper parsing of URL	N/A	O-HIR-HIOS-270420/243

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arguments. An attacker could exploit this vulnerability by specially crafting HTTP requests to overflow an internal buffer. The following devices using HiOS Version 07.0.02 and lower are affected: RSP, RSPE, RSPS, RSPL, MSP, EES, EES, EESX, GRS, OS, RED. The following devices using HiSecOS Version 03.2.00 and lower are affected: EAGLE20/30. **CVE ID : CVE-2020-6994**		
hisecos					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-04-2020	7.5	A buffer overflow vulnerability was found in some devices of Hirschmann Automation and Control HiOS and HiSecOS. The vulnerability is due to improper parsing of URL arguments. An attacker could exploit this vulnerability by specially crafting HTTP requests to overflow an internal buffer. The following devices using HiOS Version 07.0.02 and lower are affected: RSP, RSPE, RSPS, RSPL, MSP, EES, EES, EESX, GRS, OS, RED. The following devices using HiSecOS Version 03.2.00 and lower are affected: EAGLE20/30.	N/A	O-HIR-HISE-270420/244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-6994		
hms-networks					
ewon_flexy_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-04-2020	4.3	A non-persistent XSS (cross-site scripting) vulnerability exists in eWON Flexy and Cosy (all firmware versions prior to 14.1s0). An attacker could send a specially crafted URL to initiate a password change for the device. The target must introduce the credentials to the gateway before the attack can be successful. **CVE ID : CVE-2020-10633**	N/A	O-HMS-EWON-270420/245
ewon_cosy_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-04-2020	4.3	A non-persistent XSS (cross-site scripting) vulnerability exists in eWON Flexy and Cosy (all firmware versions prior to 14.1s0). An attacker could send a specially crafted URL to initiate a password change for the device. The target must introduce the credentials to the gateway before the attack can be successful. **CVE ID : CVE-2020-10633**	N/A	O-HMS-EWON-270420/246
Huawei					
mate_30_pro_firmware					
Information Exposure	10-04-2020	4.3	There is an improper authentication	N/A	O-HUA-MATE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in several smartphones. Certain function interface in the system does not sufficiently validate the caller's identity in certain share scenario, successful exploit could cause information disclosure. Affected product versions include:Mate 30 Pro versions Versions earlier than 10.0.0.205(C00E202R7P2);Mate 30 versions Versions earlier than 10.0.0.205(C00E201R7P2). **CVE ID : CVE-2020-1801**		270420/247
smartax_ma5600t_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-04-2020	5.2	There is a buffer overflow vulnerability in some Huawei products. The vulnerability can be exploited by an attacker to perform remote code execution on the affected products when the affected product functions as an optical line terminal (OLT). Affected product versions include:SmartAX MA5600T versions V800R013C10, V800R015C00, V800R015C10, V800R017C00, V800R017C10, V800R018C00, V800R018C10; SmartAX	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200401-01-overflow-en	O-HUA-SMAR-270420/248

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MA5800 versions V100R017C00, V100R017C10, V100R018C00, V100R018C10, V100R019C10; SmartAX EA5800 versions V100R018C00, V100R018C10, V100R019C10. **CVE ID : CVE-2020-9067**		
smartax_ma5800_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-04-2020	5.2	There is a buffer overflow vulnerability in some Huawei products. The vulnerability can be exploited by an attacker to perform remote code execution on the affected products when the affected product functions as an optical line terminal (OLT). Affected product versions include:SmartAX MA5600T versions V800R013C10, V800R015C00, V800R015C10, V800R017C00, V800R017C10, V800R018C00, V800R018C10; SmartAX MA5800 versions V100R017C00, V100R017C10, V100R018C00, V100R018C10, V100R019C10; SmartAX EA5800 versions V100R018C00,	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200401-01-overflow-en	O-HUA-SMAR-270420/249

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V100R018C10, V100R019C10. **CVE ID : CVE-2020-9067**		
smartax_ea5800_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-04-2020	5.2	There is a buffer overflow vulnerability in some Huawei products. The vulnerability can be exploited by an attacker to perform remote code execution on the affected products when the affected product functions as an optical line terminal (OLT). Affected product versions include:SmartAX MA5600T versions V800R013C10, V800R015C00, V800R015C10, V800R017C00, V800R017C10, V800R018C00, V800R018C10; SmartAX MA5800 versions V100R017C00, V100R017C10, V100R018C00, V100R018C10, V100R019C10; SmartAX EA5800 versions V100R018C00, V100R018C10, V100R019C10. **CVE ID : CVE-2020-9067**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200401-01-overflow-en	O-HUA-SMAR-270420/250
osca-550_firmware					
Improper Validation of Integrity Check	10-04-2020	2.1	There is an insufficient integrity validation vulnerability in several	N/A	O-HUA-OSCA-270420/251

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Value			products. The device does not sufficiently validate the integrity of certain file in certain loading processes, successful exploit could allow the attacker to load a crafted file to the device through USB.Affected product versions include:OSCA-550 versions 1.0.1.23(SP2);OSCA-550A versions 1.0.1.23(SP2);OSCA-550AX versions 1.0.1.23(SP2);OSCA-550X versions 1.0.1.23(SP2). **CVE ID : CVE-2020-1802**		
osca-550a_firmware					
Improper Validation of Integrity Check Value	10-04-2020	2.1	There is an insufficient integrity validation vulnerability in several products. The device does not sufficiently validate the integrity of certain file in certain loading processes, successful exploit could allow the attacker to load a crafted file to the device through USB.Affected product versions include:OSCA-550 versions 1.0.1.23(SP2);OSCA-550A versions 1.0.1.23(SP2);OSCA-550AX versions 1.0.1.23(SP2);OSCA-550X versions 1.0.1.23(SP2). **CVE ID : CVE-2020-1802**	N/A	O-HUA-OSCA-270420/252

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
osca-550ax_firmware					
Improper Validation of Integrity Check Value	10-04-2020	2.1	There is an insufficient integrity validation vulnerability in several products. The device does not sufficiently validate the integrity of certain file in certain loading processes, successful exploit could allow the attacker to load a crafted file to the device through USB.Affected product versions include:OSCA-550 versions 1.0.1.23(SP2);OSCA-550A versions 1.0.1.23(SP2);OSCA-550AX versions 1.0.1.23(SP2);OSCA-550X versions 1.0.1.23(SP2). **CVE ID : CVE-2020-1802**	N/A	O-HUA-OSCA-270420/253
osca-550x_firmware					
Improper Validation of Integrity Check Value	10-04-2020	2.1	There is an insufficient integrity validation vulnerability in several products. The device does not sufficiently validate the integrity of certain file in certain loading processes, successful exploit could allow the attacker to load a crafted file to the device through USB.Affected product versions include:OSCA-550 versions 1.0.1.23(SP2);OSCA-550A versions 1.0.1.23(SP2);OSCA-	N/A	O-HUA-OSCA-270420/254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			550AX versions 1.0.1.23(SP2);OSCA-550X versions 1.0.1.23(SP2). **CVE ID : CVE-2020-1802**		
mate_30_firmware					
Information Exposure	10-04-2020	4.3	There is an improper authentication vulnerability in several smartphones. Certain function interface in the system does not sufficiently validate the caller's identity in certain share scenario, successful exploit could cause information disclosure. Affected product versions include:Mate 30 Pro versions Versions earlier than 10.0.0.205(C00E202R7P2);Mate 30 versions Versions earlier than 10.0.0.205(C00E201R7P2). **CVE ID : CVE-2020-1801**	N/A	O-HUA-MATE-270420/255
ixsystems					
freenas_firmware					
Improper Authentication	08-04-2020	5	An issue was discovered in iXsystems FreeNAS (and TrueNAS) 11.2 before 11.2-u8 and 11.3 before 11.3-U1. It allows a denial of service. The login authentication component has no limits on the length of an authentication message or the rate at which such	https://security.ixsystems.com/cves/2020-04-08-cve-2020-11650/	O-IXS-FREE-270420/256

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			messages are sent. **CVE ID : CVE-2020-11650**		
truenas_firmware					
Improper Authentication	08-04-2020	5	An issue was discovered in iXsystems FreeNAS (and TrueNAS) 11.2 before 11.2-u8 and 11.3 before 11.3-U1. It allows a denial of service. The login authentication component has no limits on the length of an authentication message or the rate at which such messages are sent. **CVE ID : CVE-2020-11650**	https://security.ixsystems.com/cves/2020-04-08-cve-2020-11650/	O-IXS-TRUE-270420/257
Juniper					
junos					
Improper Authentication	08-04-2020	6.9	On Juniper Networks EX and QFX Series, an authentication bypass vulnerability may allow a user connected to the console port to login as root without any password. This issue might only occur in certain scenarios: • At the first reboot after performing device factory reset using the command "request system zeroize"; or • A temporary moment during the first reboot after the software upgrade when the device configured in Virtual	https://kb.juniper.net/JSA11001	O-JUN-JUNO-270420/258

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Chassis mode. This issue affects Juniper Networks Junos OS on EX and QFX Series: 14.1X53 versions prior to 14.1X53-D53; 15.1 versions prior to 15.1R7-S4; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S4; 17.1 versions prior to 17.1R2-S11, 17.1R3-S1; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S6; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S8; 18.2 versions prior to 18.2R2; 18.3 versions prior to 18.3R1-S7, 18.3R2. This issue does not affect Juniper Networks Junos OS 12.3. **CVE ID : CVE-2020-1618**		
Improper Privilege Management	08-04-2020	4.6	A privilege escalation vulnerability in Juniper Networks QFX10K Series, EX9200 Series, MX Series, and PTX Series with Next-Generation Routing Engine (NG-RE), allows a local authenticated high privileged user to access the underlying WRL host. This issue only affects QFX10K Series with NG-RE, EX9200 Series with NG-RE, MX Series with NG-RE and PTX Series with NG-RE; which uses	https://kb.juniper.net/JSA11002	O-JUN-JUNO-270420/259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vmhost. This issue affects Juniper Networks Junos OS: 16.1 versions prior to 16.1R7-S6; 16.2 versions prior to 16.2R2-S11; 17.1 versions prior to 17.1R2-S11, 17.1R3; 17.2 versions prior to 17.2R1-S9, 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S7, 17.4R3; 18.1 versions prior to 18.1R3-S4; 18.2 versions prior to 18.2R3; 18.2X75 versions prior to 18.2X75-D50; 18.3 versions prior to 18.3R2; 18.4 versions prior to 18.4R2. To identify whether the device has NG-RE with vmhost, customer can run the following command: > show vmhost status Compute cluster: rainier-re-cc Compute Node: rainier-re-cn, Online If the "show vmhost status" is not supported, then the device does not have NG-RE with vmhost. **CVE ID : CVE-2020-1619**		
Uncontrolled Resource Consumption	08-04-2020	3.3	The kernel memory usage represented as "temp" via 'show system virtual-memory' may constantly increase when Integrated Routing and Bridging (IRB) is configured with multiple underlay	https://kb.juniper.net/JSA11004	O-JUN-JUNO-270420/260

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			physical interfaces, and one interface flaps. This memory leak can affect running daemons (processes), leading to an extended Denial of Service (DoS) condition. Usage of "temp" virtual memory, shown here by a constantly increasing value of outstanding Requests, can be monitored by executing the 'show system virtual-memory' command as shown below: user@junos> show system virtual-memory |match "fpc|type|temp" fpc0: ---------- ---------- Type InUse MemUse HighUse Requests Size(s) temp 2023 431K - 10551 16,32,64,128,256,512,1024,2048,4096,65536,262144,1048576,2097152,4194304,8388608 fpc1: ---------- ---------- - Type InUse MemUse HighUse Requests Size(s) temp 2020 431K - 6460 16,32,64,128,256,512,1024,2048,4096,65536,262144,1048576,2097152,4194304,8388608 user@junos> show system virtual-memory |match "fpc|type|temp"		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			fpc0: ---------- ---------- ---------- Type InUse MemUse HighUse Requests Size(s) temp 2023 431K - 16101 16,32,64,128,256,512,1024,2048,4096,65536,262144,1048576,2097152,4194304,8388608 fpc1: ---------- ---------- - Type InUse MemUse HighUse Requests Size(s) temp 2020 431K - 6665 16,32,64,128,256,512,1024,2048,4096,65536,262144,1048576,2097152,4194304,8388608 user@junos> show system virtual-memory |match "fpc|type|temp" fpc0: ---------- ---------- ---------- Type InUse MemUse HighUse Requests Size(s) temp 2023 431K - 21867 16,32,64,128,256,512,1024,2048,4096,65536,262144,1048576,2097152,4194304,8388608 fpc1: ---------- ---------- - Type InUse MemUse HighUse Requests Size(s) temp 2020 431K - 6858 16,32,64,128,256,512,1024,2048,4096,65536,262144,1048576,2097152,4194304,8388608 This issue		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affects Juniper Networks Junos OS: 16.1 versions prior to 16.1R7-S6; 17.1 versions prior to 17.1R2-S11, 17.1R3-S1; 17.2 versions prior to 17.2R2-S8, 17.2R3-S3; 17.2X75 versions prior to 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S6; 17.4 versions prior to 17.4R2-S5, 17.4R3; 18.1 versions prior to 18.1R3-S7; 18.2 versions prior to 18.2R2-S5, 18.2R3; 18.2X75 versions prior to 18.2X75-D33, 18.2X75-D411, 18.2X75-D420, 18.2X75-D60; 18.3 versions prior to 18.3R1-S5, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R2-S2, 18.4R3; 19.1 versions prior to 19.1R1-S3, 19.1R2; 19.2 versions prior to 19.2R1-S3, 19.2R2. This issue does not affect Juniper Networks Junos OS 12.3 and 15.1. **CVE ID : CVE-2020-1625**		
Improper Input Validation	08-04-2020	5	A vulnerability in Juniper Networks Junos OS on vMX and MX150 devices may allow an attacker to cause a Denial of Service (DoS) by sending specific packets requiring special processing in microcode that the flow cache can't handle, causing the riot	https://kb.juniper.net/JSA11006	O-JUN-JUNO-270420/261

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			forwarding daemon to crash. By continuously sending the same specific packets, an attacker can repeatedly crash the riot process causing a sustained Denial of Service. Flow cache is specific to vMX based products and the MX150, and is enabled by default in performance mode. This issue can only be triggered by traffic destined to the device. Transit traffic will not cause the riot daemon to crash. When the issue occurs, a core dump and riot log file entry are generated. For example: /var/crash/core.J-UKERN.mpc0.1557255993.3864.gz /home/pfe/RIOT logs: fpc0 riot[1888]: PANIC in lu_reorder_send_packet_postproc(): fpc0 riot[6655]: PANIC in lu_reorder_send_packet_postproc(): This issue affects Juniper Networks Junos OS: 18.1 versions prior to 18.1R3 on vMX and MX150; 18.2 versions prior to 18.2R3 on vMX and MX150; 18.2X75 versions prior to 18.2X75-D60 on vMX and MX150; 18.3 versions prior to 18.3R3 on vMX and		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MX150; 18.4 versions prior to 18.4R2 on vMX and MX150; 19.1 versions prior to 19.1R2 on vMX and MX150. This issue does not affect Junos OS versions prior to 18.1R1. **CVE ID : CVE-2020-1627**		
Information Exposure	08-04-2020	5	Juniper Networks Junos OS uses the 128.0.0.0/2 subnet for internal communications between the RE and PFEs. It was discovered that packets utilizing these IP addresses may egress an EX4300 switch, leaking configuration information such as heartbeats, kernel versions, etc. out to the Internet, leading to an information exposure vulnerability. This issue affects Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D53 on EX4300; 15.1 versions prior to 15.1R7-S6 on EX4300; 15.1X49 versions prior to 15.1X49-D200, 15.1X49-D210 on EX4300; 16.1 versions prior to 16.1R7-S7 on EX4300; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2 on EX4300; 17.2 versions prior to 17.2R3-S3 on EX4300; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7 on EX4300; 17.4 versions	https://kb.juniper.net/JSA11008	O-JUN-JUNO-270420/262

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 17.4R2-S9, 17.4R3 on EX4300; 18.1 versions prior to 18.1R3-S8 on EX4300; 18.2 versions prior to 18.2R3-S2 on EX4300; 18.3 versions prior to 18.3R2-S3, 18.3R3, 18.3R3-S1 on EX4300; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R3 on EX4300; 19.1 versions prior to 19.1R1-S4, 19.1R2 on EX4300; 19.2 versions prior to 19.2R1-S4, 19.2R2 on EX4300; 19.3 versions prior to 19.3R1-S1, 19.3R2 on EX4300. **CVE ID : CVE-2020-1628**		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-04-2020	4.3	A race condition vulnerability on Juniper Network Junos OS devices may cause the routing protocol daemon (RPD) process to crash and restart while processing a BGP NOTIFICATION message. This issue affects Juniper Networks Junos OS: 16.1 versions prior to 16.1R7-S6; 16.2 versions prior to 16.2R2-S11; 17.1 versions prior to 17.1R2-S11, 17.1R3-S1; 17.2 versions prior to 17.2R1-S9, 17.2R3-S3; 17.2 version 17.2R2 and later versions; 17.2X75 versions prior to 17.2X75-D105, 17.2X75-D110;	https://kb.juniper.net/JSA11009	O-JUN-JUNO-270420/263

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			17.3 versions prior to 17.3R2-S5, 17.3R3-S6; 17.4 versions prior to 17.4R2-S7, 17.4R3; 18.1 versions prior to 18.1R3-S8; 18.2 versions prior to 18.2R3-S3; 18.2X75 versions prior to 18.2X75-D410, 18.2X75-D420, 18.2X75-D50, 18.2X75-D60; 18.3 versions prior to 18.3R1-S5, 18.3R2-S2, 18.3R3; 18.4 versions prior to 18.4R2-S2, 18.4R3; 19.1 versions prior to 19.1R1-S2, 19.1R2; 19.2 versions prior to 19.2R1-S4, 19.2R2. This issue does not affect Juniper Networks Junos OS prior to version 16.1R1. **CVE ID : CVE-2020-1629**		
Improper Privilege Management	08-04-2020	2.1	A privilege escalation vulnerability in Juniper Networks Junos OS devices configured with dual Routing Engines (RE), Virtual Chassis (VC) or high-availability cluster may allow a local authenticated low-privileged user with access to the shell to perform unauthorized configuration modification. This issue does not affect Junos OS device with single RE or stand-alone configuration. This issue affects Juniper	https://kb.juniper.net/JSA11010	O-JUN-JUNO-270420/264

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS 12.3 versions prior to 12.3R12-S14; 12.3X48 versions prior to 12.3X48-D86, 12.3X48-D90; 14.1X53 versions prior to 14.1X53-D51; 15.1 versions prior to 15.1R7-S6; 15.1X49 versions prior to 15.1X49-D181, 15.1X49-D190; 15.1X53 versions prior to 15.1X53-D592; 16.1 versions prior to 16.1R4-S13, 16.1R7-S6; 16.2 versions prior to 16.2R2-S10; 17.1 versions prior to 17.1R2-S11, 17.1R3-S1; 17.2 versions prior to 17.2R1-S9, 17.2R3-S3; 17.3 versions prior to 17.3R3-S6; 17.4 versions prior to 17.4R2-S6, 17.4R3; 18.1 versions prior to 18.1R3-S7; 18.2 versions prior to 18.2R2-S5, 18.2R3-S1; 18.2 versions prior to 18.2X75-D12, 18.2X75-D33, 18.2X75-D420, 18.2X75-D60, 18.2X75-D411; 18.3 versions prior to 18.3R1-S5, 18.3R2-S1, 18.3R3; 18.4 versions prior to 18.4R1-S4, 18.4R2-S1, 18.4R3; 19.1 versions prior to 19.1R1-S2, 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2020-1630**		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	09-04-2020	3.3	Due to a new NDP proxy feature for EVPN leaf nodes introduced in Junos OS 17.4, crafted NDPv6 packets could transit a Junos device configured as a Broadband Network Gateway (BNG) and reach the EVPN leaf node, causing a stale MAC address entry. This could cause legitimate traffic to be discarded, leading to a Denial of Service (DoS) condition. This issue only affects Junos OS 17.4 and later releases. Prior releases do not support this feature and are unaffected by this vulnerability. This issue only affects IPv6. IPv4 ARP proxy is unaffected by this vulnerability. This issue affects Juniper Networks Junos OS: 17.4 versions prior to 17.4R2-S9, 17.4R3 on MX Series; 18.1 versions prior to 18.1R3-S9 on MX Series; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D33, 18.2X75-D411, 18.2X75-D420, 18.2X75-D60 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3 on MX Series; 18.4 versions prior to 18.4R1-S5,	https://kb.juniper.net/JSA11012	O-JUN-JUNO-270420/265

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.4R2-S2, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2 on MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series. **CVE ID : CVE-2020-1633**		
Improper Input Validation	08-04-2020	4.3	On High-End SRX Series devices, in specific configurations and when specific networking events or operator actions occur, an SPC receiving genuine multicast traffic may core. Subsequently, all FPCs in a chassis may reset causing a Denial of Service. This issue affects both IPv4 and IPv6. This issue affects: Juniper Networks Junos OS 12.3X48 version 12.3X48-D80 and later versions prior to 12.3X48-D95 on High-End SRX Series. This issue does not affect Branch SRX Series devices. **CVE ID : CVE-2020-1634**	N/A	O-JUN-JUNO-270420/266
Improper Authentication	08-04-2020	5.8	A vulnerability in Juniper Networks SRX Series device configured as a Junos OS Enforcer device may allow a user to access network resources that are not permitted by a UAC policy. This issue might occur when the IP address range configured in the Infranet Controller	https://kb.juniper.net/JSA11018	O-JUN-JUNO-270420/267

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(IC) is configured as an IP address range instead of an IP address/netmask. See the Workaround section for more detail. The Junos OS Enforcer CLI settings are disabled by default. This issue affects Juniper Networks Junos OS on SRX Series: 12.3X48 versions prior to 12.3X48-D100; 15.1X49 versions prior to 15.1X49-D210; 17.3 versions prior to 17.3R2-S5, 17.3R3-S8; 17.4 versions prior to 17.4R2-S9, 17.4R3-S1; 18.1 versions prior to 18.1R3-S10; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R3-S2; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3-S1; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S3, 19.2R2; 19.3 versions prior to 19.3R2-S1, 19.3R3; 19.4 versions prior to 19.4R1-S1, 19.4R2. **CVE ID : CVE-2020-1637**		
Improper Input Validation	08-04-2020	5	The FPC (Flexible PIC Concentrator) of Juniper Networks Junos OS and Junos OS Evolved may restart after processing a specific IPv4 packet. Only	https://kb.juniper.net/JSA11019	O-JUN-JUNO-270420/268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			packets destined to the device itself, successfully reaching the RE through existing edge and control plane filtering, will be able to cause the FPC restart. When this issue occurs, all traffic via the FPC will be dropped. By continuously sending this specific IPv4 packet, an attacker can repeatedly crash the FPC, causing an extended Denial of Service (DoS) condition. This issue can only occur when processing a specific IPv4 packet. IPv6 packets cannot trigger this issue. This issue affects: Juniper Networks Junos OS on MX Series with MPC10E or MPC11E and PTX10001: 19.2 versions prior to 19.2R1-S4, 19.2R2; 19.3 versions prior to 19.3R2-S2, 19.3R3; 19.4 versions prior to 19.4R1-S1, 19.4R2. Juniper Networks Junos OS Evolved on on QFX5220, and PTX10003 series: 19.2-EVO versions; 19.3-EVO versions; 19.4-EVO versions prior to 19.4R2-EVO. This issue does not affect Junos OS versions prior to 19.2R1. This issue does not affect Junos OS Evolved versions prior to 19.2R1-EVO.		

CVSS Scoring Scale	0-1	1-2	2-3	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-2020-1638		
Improper Handling of Exceptional Conditions	08-04-2020	5	When an attacker sends a specific crafted Ethernet Operation, Administration, and Maintenance (Ethernet OAM) packet to a target device, it may improperly handle the incoming malformed data and fail to sanitize this incoming data resulting in an overflow condition. This overflow condition in Juniper Networks Junos OS allows an attacker to cause a Denial of Service (DoS) condition by coring the CFM daemon. Continued receipt of these packets may cause an extended Denial of Service condition. This issue affects: Juniper Networks Junos OS 12.3 versions prior to 12.3R12-S15; 12.3X48 versions prior to 12.3X48-D95 on SRX Series; 14.1X50 versions prior to 14.1X50-D145; 14.1X53 versions prior to 14.1X53-D47; 15.1 versions prior to 15.1R2; 15.1X49 versions prior to 15.1X49-D170 on SRX Series; 15.1X53 versions prior to 15.1X53-D67. **CVE ID : CVE-2020-1639**	N/A	O-JUN-JUNO-270420/269
Improper	08-04-2020	5	A vulnerability in the BGP	https://kb.j	O-JUN-JUNO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX	uniper.net/JSA10996	270420/270

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
Use of Hard-coded Credentials	08-04-2020	9.3	A Use of Hard-coded Credentials vulnerability exists in the NFX250 Series for the vSRX Virtual Network Function (VNF) instance, which allows an attacker to take control of the vSRX VNF instance if they have the ability to access an administrative service (e.g. SSH) on the VNF, either locally, or through the network. This issue only affects the NFX250 Series vSRX VNF. No other products or platforms are affected. This issue is only applicable to environments where the vSRX VNF root password has not been configured.	N/A	O-JUN-JUNO-270420/271

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This issue affects the Juniper Networks NFX250 Network Services Platform vSRX VNF instance on versions prior to 19.2R1. **CVE ID : CVE-2020-1614**		
Use of Hard-coded Credentials	08-04-2020	10	The factory configuration for vMX installations, as shipped, includes default credentials for the root account. Without proper modification of these default credentials by the administrator, an attacker could exploit these credentials and access the vMX instance without authorization. This issue affects Juniper Networks Junos OS: 17.1 versions prior to 17.1R2-S11, 17.1R3-S2 on vMX; 17.2 versions prior to 17.2R3-S3 on vMX; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7 on vMX; 17.4 versions prior to 17.4R2-S9, 17.4R3 on vMX; 18.1 versions prior to 18.1R3-S9 on vMX; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3 on vMX; 18.2X75 versions prior to 18.2X75-D420, 18.2X75-D60 on vMX; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1 on vMX; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R3 on	https://kb.juniper.net/JSA10998	O-JUN-JUNO-270420/272

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vMX; 19.1 versions prior to 19.1R1-S4, 19.1R2, 19.1R3 on vMX; 19.2 versions prior to 19.2R1-S3, 19.2R2 on vMX; 19.3 versions prior to 19.3R1-S1, 19.3R2 on vMX. **CVE ID : CVE-2020-1615**		
Improper Initialization	08-04-2020	7.8	This issue occurs on Juniper Networks Junos OS devices which do not support Advanced Forwarding Interface (AFI) / Advanced Forwarding Toolkit (AFT). Devices using AFI and AFT are not exploitable to this issue. An improper initialization of memory in the packet forwarding architecture in Juniper Networks Junos OS non-AFI/AFT platforms which may lead to a Denial of Service (DoS) vulnerability being exploited when a genuine packet is received and inspected by non-AFT/AFI sFlow and when the device is also configured with firewall policers. This first genuine packet received and inspected by sampled flow (sFlow) through a specific firewall policer will cause the device to reboot. After the reboot has completed, if the device receives and sFlow	N/A	O-JUN-JUNO-270420/273

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			inspects another genuine packet seen through a specific firewall policer, the device will generate a core file and reboot. Continued inspection of these genuine packets will create an extended Denial of Service (DoS) condition. Depending on the method for service restoration, e.g. hard boot or soft reboot, a core file may or may not be generated the next time the packet is received and inspected by sFlow. This issue affects: Juniper Networks Junos OS 17.4 versions prior to 17.4R2-S9, 17.4R3 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.1 versions prior to 18.1R3-S9 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.2X75 versions prior to 18.2X75-D12, 18.2X75-D30 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.2 versions prior to 18.2R3 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.3 versions prior to 18.3R3 on PTX1000 and PTX10000 Series, QFX10000 Series. This issue is not applicable 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
			Junos OS versions before 17.4R1. This issue is not applicable to Junos OS Evolved or Junos OS with Advanced Forwarding Toolkit (AFT) forwarding implementations which use a different implementation of sFlow. The following example information is unrelated to this issue and is provided solely to assist you with determining if you have AFT or not. Example: A Junos OS device which supports the use of EVPN signaled VPWS with Flexible Cross Connect uses the AFT implementation. Since this configuration requires support and use of the AFT implementation to support this configuration, the device is not vulnerable to this issue as the sFlow implementation is different using the AFT architecture. For further details about AFT visit the AFI / AFT are in the links below. If you are uncertain if you use the AFI/AFT implementation or not, there are configuration examples in the links below which you may use to determine if		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			you are vulnerable to this issue or not. If the commands work, you are. If not, you are not. You may also use the Feature Explorer to determine if AFI/AFT is supported or not. If you are still uncertain, please contact your support resources. **CVE ID : CVE-2020-1617**		
junos_os_evolved					
Information Exposure Through Log Files	08-04-2020	2.1	A local, authenticated user with shell can obtain the hashed values of login passwords via configd streamer log. This issue affects all versions of Junos OS Evolved prior to 19.3R1. **CVE ID : CVE-2020-1620**	https://kb.juniper.net/JSA11003	O-JUN-JUNO-270420/274
Information Exposure Through Log Files	08-04-2020	2.1	A local, authenticated user with shell can obtain the hashed values of login passwords via configd traces. This issue affects all versions of Junos OS Evolved prior to 19.3R1. **CVE ID : CVE-2020-1621**	https://kb.juniper.net/JSA11003	O-JUN-JUNO-270420/275
Information Exposure Through Log Files	08-04-2020	2.1	A local, authenticated user with shell can obtain the hashed values of login passwords and shared secrets via the EvoSharedObjStore. This issue affects all versions of Junos OS Evolved prior to 19.1R1.	https://kb.juniper.net/JSA11003	O-JUN-JUNO-270420/276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1622		
Information Exposure Through Log Files	08-04-2020	2.1	A local, authenticated user with shell can view sensitive configuration information via the ev.ops configuration file. This issue affects all versions of Junos OS Evolved prior to 19.2R1. **CVE ID : CVE-2020-1623**	https://kb.juniper.net/JSA11003	O-JUN-JUNO-270420/277
Information Exposure Through Log Files	08-04-2020	2.1	A local, authenticated user with shell can obtain the hashed values of login passwords and shared secrets via raw objmon configuration files. This issue affects all versions of Junos OS Evolved prior to 19.1R1. **CVE ID : CVE-2020-1624**	https://kb.juniper.net/JSA11003	O-JUN-JUNO-270420/278
junos_evolved					
Improper Input Validation	08-04-2020	5	The FPC (Flexible PIC Concentrator) of Juniper Networks Junos OS and Junos OS Evolved may restart after processing a specific IPv4 packet. Only packets destined to the device itself, successfully reaching the RE through existing edge and control plane filtering, will be able to cause the FPC restart. When this issue occurs, all traffic via the FPC will be dropped. By continuously sending this specific IPv4 packet, an attacker can repeatedly	https://kb.juniper.net/JSA11019	O-JUN-JUNO-270420/279

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crash the FPC, causing an extended Denial of Service (DoS) condition. This issue can only occur when processing a specific IPv4 packet. IPv6 packets cannot trigger this issue. This issue affects: Juniper Networks Junos OS on MX Series with MPC10E or MPC11E and PTX10001: 19.2 versions prior to 19.2R1-S4, 19.2R2; 19.3 versions prior to 19.3R2-S2, 19.3R3; 19.4 versions prior to 19.4R1-S1, 19.4R2. Juniper Networks Junos OS Evolved on on QFX5220, and PTX10003 series: 19.2-EVO versions; 19.3-EVO versions; 19.4-EVO versions prior to 19.4R2-EVO. This issue does not affect Junos OS versions prior to 19.2R1. This issue does not affect Junos OS Evolved versions prior to 19.2R1-EVO. **CVE ID : CVE-2020-1638**		
Linux					
linux_kernel					
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-04-2020	7.2	In the Linux kernel 5.5.0 and newer, the bpf verifier (kernel/bpf/verifier.c) did not properly restrict the register bounds for 32-bit operations, leading to out-of-bounds reads	https://git.kernel.org/pub/scm/linux/kernel/git/netdev/net-next.git/commit/?id=f	O-LIN-LINU-270420/280

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and writes in kernel memory. The vulnerability also affects the Linux 5.4 stable series, starting with v5.4.7, as the introducing commit was backported to that branch. This vulnerability was fixed in 5.6.1, 5.5.14, and 5.4.29. (issue is aka ZDI-CAN-10780) **CVE ID : CVE-2020-8835**	2d67fec0b43edce8c416101cdc52e71145b5fef, https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=f2d67fec0b43edce8c416101cdc52e71145b5fef	
Information Exposure	02-04-2020	2.1	An issue was discovered in slc_bump in drivers/net/can/slcan.c in the Linux kernel through 5.6.2. It allows attackers to read uninitialized can_frame data, potentially containing sensitive information from kernel stack memory, if the configuration lacks CONFIG_INIT_STACK_ALL, aka CID-b9258a2cece4. **CVE ID : CVE-2020-11494**	N/A	O-LIN-LINU-270420/281
Out-of-bounds Write	06-04-2020	4.6	An issue was discovered in the Linux kernel through 5.6.2. mpol_parse_str in mm/mempolicy.c has a stack-based out-of-bounds write because an empty nodelist is	N/A	O-LIN-LINU-270420/282

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mishandled during mount option parsing, aka CID-aa9f7d5172fa. **CVE ID : CVE-2020-11565**		
Improper Certificate Validation	06-04-2020	6.4	An issue was discovered in Pulse Secure Pulse Connect Secure (PCS) through 2020-04-06. The applet in tncc.jar, executed on macOS, Linux, and Solaris clients when a Host Checker policy is enforced, accepts an arbitrary SSL certificate. **CVE ID : CVE-2020-11580**	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44426	O-LIN-LINU-270420/283
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-04-2020	9.3	An issue was discovered in Pulse Secure Pulse Connect Secure (PCS) through 2020-04-06. The applet in tncc.jar, executed on macOS, Linux, and Solaris clients when a Host Checker policy is enforced, allows a man-in-the-middle attacker to perform OS command injection attacks (against a client) via shell metacharacters to the doCustomRemediateInstructions method, because Runtime.getRuntime().exec() is used. **CVE ID : CVE-2020-11581**	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44426	O-LIN-LINU-270420/284

CVSS Scoring Scale	0-1	1-2	2-3	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 Excessive Authentication Attempts	06-04-2020	3.3	An issue was discovered in Pulse Secure Pulse Connect Secure (PCS) through 2020-04-06. The applet in tncc.jar, executed on macOS, Linux, and Solaris clients when a Host Checker policy is enforced, launches a TCP server that accepts local connections on a random port. This can be reached by local HTTP clients, because up to 25 invalid lines are ignored, and because DNS rebinding can occur. (This server accepts, for example, a setcookie command that might be relevant to CVE-2020-11581 exploitation.) **CVE ID : CVE-2020-11582**	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44426	O-LIN-LINU-270420/285
NULL Pointer Dereference	07-04-2020	2.1	An issue was discovered in the Linux kernel before 5.6.1. drivers/media/usb/gspca/ov519.c allows NULL pointer dereferences in ov511_mode_init_regs and ov518_mode_init_regs when there are zero endpoints, aka CID-998912346c0d. **CVE ID : CVE-2020-11608**	N/A	O-LIN-LINU-270420/286
NULL Pointer	07-04-2020	4.9	An issue was discovered	N/A	O-LIN-LINU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			in the stv06xx subsystem in the Linux kernel before 5.6.1. drivers/media/usb/gspca/stv06xx/stv06xx.c and drivers/media/usb/gspca/stv06xx/stv06xx_pb0100.c mishandle invalid descriptors, as demonstrated by a NULL pointer dereference, aka CID-485b06aadb93. **CVE ID : CVE-2020-11609**		270420/287
Improper Input Validation	09-04-2020	5	In the Linux kernel before 5.6.1, drivers/media/usb/gspca/xirlink_cit.c (aka the Xirlink camera USB driver) mishandles invalid descriptors, aka CID-a246b4d54770. **CVE ID : CVE-2020-11668**	N/A	O-LIN-LINU-270420/288
N/A	10-04-2020	5	An issue was discovered in the Linux kernel before 5.2 on the powerpc platform. arch/powerpc/kernel/idle_book3s.S does not have save/restore functionality for PNV_POWERSAVE_AMR, PNV_POWERSAVE_UAMOR, and PNV_POWERSAVE_AMOR, aka CID-53a712bae5dd. **CVE ID : CVE-2020-11669**	N/A	O-LIN-LINU-270420/289

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	12-04-2020	4.6	** DISPUTED ** snd_ctl_elem_add in sound/core/control.c in the Linux kernel through 5.6.3 has a count=info->owner line, which later affects a private_size*count multiplication for unspecified "interesting side effects." NOTE: kernel engineers dispute this finding, because it could be relevant only if new callers were added that were unfamiliar with the misuse of the info->owner field to represent data unrelated to the "owner" concept. The existing callers, SNDRV_CTL_IOCTL_ELEM_ADD and SNDRV_CTL_IOCTL_ELEM_REPLACE, have been designed to misuse the info->owner field in a safe way. **CVE ID : CVE-2020-11725**	N/A	O-LIN-LINU-270420/290
mi					
xiaomi_xiaoai_speaker_pro_lx06_firmware					
Improper Input Validation	08-04-2020	7.2	An issue was discovered on XIAOMI XIAOAI speaker Pro LX06 1.58.10. Attackers can activate the failsafe mode during the boot process, and use the mi_console command cascaded by the SN code	N/A	O-MI-XIAO-270420/291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			shown on the product to get the root shell password, and then the attacker can (i) read Wi-Fi SSID or password, (ii) read the dialogue text files between users and XIAOMI XIAOAI speaker Pro LX06, (iii) use Text-To-Speech tools pretend XIAOMI speakers' voice achieve social engineering attacks, (iv) eavesdrop on users and record what XIAOMI XIAOAI speaker Pro LX06 hears, (v) modify system files, (vi) use commands to send any IR code through IR emitter on XIAOMI XIAOAI Speaker Pro (LX06), (vii) stop voice assistant service, (viii) enable the XIAOMI XIAOAI Speaker Pro's SSH or TELNET service as a backdoor, (IX) tamper with the router configuration of the router in the local area networks. **CVE ID : CVE-2020-10262**		
Improper Input Validation	08-04-2020	7.2	An issue was discovered on XIAOMI XIAOAI speaker Pro LX06 1.52.4. Attackers can get root shell by accessing the UART interface and then they can (i) read Wi-Fi SSID or password, (ii)	N/A	O-MI-XIAO-270420/292

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			read the dialogue text files between users and XIAOMI XIAOAI speaker Pro LX06, (iii) use Text-To-Speech tools pretend XIAOMI speakers' voice achieve social engineering attacks, (iv) eavesdrop on users and record what XIAOMI XIAOAI speaker Pro LX06 hears, (v) modify system files, (vi) use commands to send any IR code through IR emitter on XIAOMI XIAOAI Speaker Pro LX06, (vii) stop voice assistant service, (viii) enable the XIAOMI XIAOAI Speaker Pro' SSH or TELNET service as a backdoor, (IX) tamper with the router configuration of the router in the local area networks. **CVE ID : CVE-2020-10263**		
Microsoft					
windows					
Uncontrolled Search Path Element	02-04-2020	10	STARFACE UCC Client before 6.7.1.204 on WIndows allows binary planting to execute code with System rights, aka usd-2020-0006. **CVE ID : CVE-2020-10515**	https://support.starface.de/forum/showthread.php?7916-UCC-Client-f%FCr-Windows-Version-6-7-1-204-	O-MIC-WIND-270420/293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				Released-26-03-2020&p=47548	
Out-of-bounds Write	01-04-2020	5	An issue was discovered in Avast Antivirus before 20. An Arbitrary Memory Address Overwrite vulnerability in the aswAvLog Log Library results in Denial of Service of the Avast Service (AvastSvc.exe). **CVE ID : CVE-2020-10860**	N/A	O-MIC-WIND-270420/294
Improper Input Validation	01-04-2020	6.4	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to achieve Arbitrary File Deletion from Avast Program Path via RPC, when Self Defense is Enabled. **CVE ID : CVE-2020-10861**	N/A	O-MIC-WIND-270420/295
Improper Privilege Management	01-04-2020	4.6	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to achieve Local Privilege Escalation (LPE) via RPC. **CVE ID : CVE-2020-**	N/A	O-MIC-WIND-270420/296

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10862		
Improper Input Validation	01-04-2020	5	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to trigger a shutdown via RPC from a Low Integrity process via TempShutDownMachine. **CVE ID : CVE-2020-10863**	N/A	O-MIC-WIND-270420/297
Improper Input Validation	01-04-2020	5	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to trigger a reboot via RPC from a Low Integrity process. **CVE ID : CVE-2020-10864**	N/A	O-MIC-WIND-270420/298
Inclusion of Functionality from Untrusted Control Sphere	01-04-2020	5	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to make arbitrary changes to the Components section of the Stats.ini file via RPC from a Low Integrity process. **CVE ID : CVE-2020-10865**	N/A	O-MIC-WIND-270420/299

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
Inadequate Encryption Strength	01-04-2020	5	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to enumerate the network interfaces and access points from a Low Integrity process via RPC. **CVE ID : CVE-2020-10866**	N/A	O-MIC-WIND-270420/300
Exposure of Resource to Wrong Sphere	01-04-2020	7.5	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to bypass intended access restrictions on tasks from an untrusted process, when Self Defense is enabled. **CVE ID : CVE-2020-10867**	N/A	O-MIC-WIND-270420/301
Incorrect Permission Assignment for Critical Resource	01-04-2020	5	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to launch the Repair App RPC call from a Low Integrity process. **CVE ID : CVE-2020-10868**	N/A	O-MIC-WIND-270420/302

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	02-04-2020	6.8	An issue was discovered in XAMPP before 7.2.29, 7.3.x before 7.3.16 , and 7.4.x before 7.4.4 on Windows. An unprivileged user can change a .exe configuration in xampp-contol.ini for all users (including admins) to enable arbitrary command execution. **CVE ID : CVE-2020-11107**	https://www.apachefriends.org/blog/new_xampp_20200401.html	O-MIC-WIND-270420/303
Insufficiently Protected Credentials	10-04-2020	5	In JetBrains PyCharm 2019.2.5 and 2019.3 on Windows, Apple Notarization Service credentials were included. This is fixed in 2019.2.6 and 2019.3.3. **CVE ID : CVE-2020-11694**	N/A	O-MIC-WIND-270420/304
Improper Input Validation	08-04-2020	7.2	Secdo tries to execute a script at a hardcoded path if present, which allows a local authenticated user with 'create folders or append data' access to the root of the OS disk (C:\) to gain system privileges if the path does not already exist or is writable. This issue affects all versions of Secdo for Windows. **CVE ID : CVE-2020-1984**	N/A	O-MIC-WIND-270420/305
Incorrect Default Permissions	08-04-2020	4.6	Incorrect Default Permissions on C:\Programdata\Secdo\L	N/A	O-MIC-WIND-270420/306

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ogs folder in Secdo allows local authenticated users to overwrite system files and gain escalated privileges. This issue affects all versions Secdo for Windows. **CVE ID : CVE-2020-1985**		
Improper Input Validation	08-04-2020	4.9	Improper input validation vulnerability in Secdo allows an authenticated local user with 'create folders or append data' access to the root of the OS disk (C:\) to cause a system crash on every login. This issue affects all versions Secdo for Windows. **CVE ID : CVE-2020-1986**	N/A	O-MIC-WIND-270420/307
Improper Privilege Management	08-04-2020	3.6	An insecure temporary file vulnerability in Palo Alto Networks Traps allows a local authenticated Windows user to escalate privileges or overwrite system files. This issue affects Palo Alto Networks Traps 5.0 versions before 5.0.8; 6.1 versions before 6.1.4 on Windows. This issue does not affect Cortex XDR 7.0. This issue does not affect Traps for Linux or MacOS. **CVE ID : CVE-2020-1991**	N/A	O-MIC-WIND-270420/308
Improper Limitation of a Pathname to a	01-04-2020	5.2	The UniFi Video Server v3.9.3 and prior (for Windows 7/8/10 x64)	https://community.ui.com/releas	O-MIC-WIND-270420/309

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			web interface Firmware Update functionality, under certain circumstances, does not validate firmware download destinations to ensure they are within the intended destination directory tree. It accepts a request with a URL to firmware update information. If the version field contains ..\ character sequences, the destination file path to save the firmware can be manipulated to be outside the intended destination directory tree. Fixed in UniFi Video Controller v3.10.3 and newer. **CVE ID : CVE-2020-8144**	es/Security-advisory-bulletin-006-006/3cf6264e-e0e6-4e26-a331-1d271f84673e	
Improper Privilege Management	01-04-2020	4	The UniFi Video Server (Windows) web interface configuration restore functionality at the "backup" and "wizard" endpoints does not implement sufficient privilege checks. Low privileged users, belonging to the PUBLIC_GROUP or CUSTOM_GROUP groups, can access these endpoints and overwrite the current application configuration. This can be abused for various purposes, including adding new	https://community.ui.com/releases/Security-advisory-bulletin-006-006/3cf6264e-e0e6-4e26-a331-1d271f84673e	O-MIC-WIND-270420/310

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			administrative users. Affected Products: UniFi Video Controller v3.9.3 (for Windows 7/8/10 x64) and prior. Fixed in UniFi Video Controller v3.9.6 and newer. **CVE ID : CVE-2020-8145**		
Improper Privilege Management	01-04-2020	6.9	In UniFi Video v3.10.1 (for Windows 7/8/10 x64) there is a Local Privileges Escalation to SYSTEM from arbitrary file deletion and DLL hijack vulnerabilities. The issue was fixed by adjusting the .tsExport folder when the controller is running on Windows and adjusting the SafeDllSearchMode in the windows registry when installing UniFi-Video controller. Affected Products: UniFi Video Controller v3.10.2 (for Windows 7/8/10 x64) and prior. Fixed in UniFi Video Controller v3.10.3 and newer. **CVE ID : CVE-2020-8146**	https://community.ui.com/releases/Security-advisory-bulletin-006-006/3cf6264e-e0e6-4e26-a331-1d271f84673e	O-MIC-WIND-270420/311
mysyngeryss					
husky_rtu_6049-e70_firmware					
Improper Check for Unusual or Exceptional Conditions	14-04-2020	8.5	The Synergy Systems & Solutions (SSS) HUSKY RTU 6049-E70, with firmware Versions 5.0 and prior, has an Improper Check for	N/A	O-MYS-HUSK-270420/312

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Unusual or Exceptional Conditions (CWE-754) vulnerability. The affected product is vulnerable to specially crafted TCP packets, which can cause the device to shut down or reboot and lose configuration settings. This is a different issue than CVE-2019-16879, CVE-2019-20045, CVE-2019-20046, CVE-2020-7801, and CVE-2020-7802. **CVE ID : CVE-2020-7800**		
Information Exposure	14-04-2020	5	The Synergy Systems & Solutions (SSS) HUSKY RTU 6049-E70, with firmware Versions 5.0 and prior, has an Exposure of Sensitive Information to an Unauthorized Actor (CWE-200) vulnerability. The affected product is vulnerable to information exposure over the SNMP protocol. This is a different issue than CVE-2019-16879, CVE-2019-20045, CVE-2019-20046, CVE-2020-7800, and CVE-2020-7802. **CVE ID : CVE-2020-7801**	N/A	O-MYS-HUSK-270420/313
Incorrect Default Permissions	14-04-2020	5	The Synergy Systems & Solutions (SSS) HUSKY RTU 6049-E70, with firmware Versions 5.0 and prior, has an	N/A	O-MYS-HUSK-270420/314

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Incorrect Default Permissions (CWE-276) vulnerability. The affected product is vulnerable to insufficient default permissions, which could allow an attacker to view network configurations through SNMP communication. This is a different issue than CVE-2019-16879, CVE-2019-20045, CVE-2019-20046, CVE-2020-7800, and CVE-2020-7801. **CVE ID : CVE-2020-7802**		
Opensuse					
opensuse					
Improper Link Resolution Before File Access ('Link Following')	02-04-2020	7.2	A UNIX Symbolic Link (Symlink) Following vulnerability in the packaging of exim in openSUSE Factory allows local attackers to escalate from user mail to root. This issue affects: openSUSE Factory exim versions prior to 4.93.0.4-3.1. **CVE ID : CVE-2020-8015**	https://bugzilla.suse.com/show_bug.cgi?id=1154183	O-OPE-OPEN-270420/315
leap					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-04-2020	4.4	A Race Condition Enabling Link Following vulnerability in the packaging of texlive-filesystem of SUSE Linux Enterprise Module for Desktop Applications 15-SP1, SUSE Linux	https://bugzilla.suse.com/show_bug.cgi?id=1159740	O-OPE-LEAP-270420/316

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Software Development Kit 12-SP4, SUSE Linux Enterprise Software Development Kit 12-SP5; openSUSE Leap 15.1 allows local users to corrupt files or potentially escalate privileges. This issue affects: SUSE Linux Enterprise Module for Desktop Applications 15-SP1 texlive-filesystem versions prior to 2017.135-9.5.1. SUSE Linux Enterprise Software Development Kit 12-SP4 texlive-filesystem versions prior to 2013.74-16.5.1. SUSE Linux Enterprise Software Development Kit 12-SP5 texlive-filesystem versions prior to 2013.74-16.5.1. openSUSE Leap 15.1 texlive-filesystem versions prior to 2017.135-lp151.8.3.1. **CVE ID : CVE-2020-8016**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-04-2020	3.3	A Race Condition Enabling Link Following vulnerability in the cron job shipped with texlive-filesystem of SUSE Linux Enterprise Module for Desktop Applications 15-SP1, SUSE Linux Enterprise Software Development Kit 12-SP4, SUSE Linux Enterprise Software Development Kit 12-SP5; openSUSE Leap	https://bugzilla.suse.com/show_bug.cgi?id=1158910	O-OPE-LEAP-270420/317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			15.1 allows local users in group mktex to delete arbitrary files on the system This issue affects: SUSE Linux Enterprise Module for Desktop Applications 15-SP1 texlive-filesystem versions prior to 2017.135-9.5.1. SUSE Linux Enterprise Software Development Kit 12-SP4 texlive-filesystem versions prior to 2013.74-16.5.1. SUSE Linux Enterprise Software Development Kit 12-SP5 texlive-filesystem versions prior to 2013.74-16.5.1. openSUSE Leap 15.1 texlive-filesystem versions prior to 2017.135-lp151.8.3.1. **CVE ID : CVE-2020-8017**		
Oracle					
solaris					
Improper Certificate Validation	06-04-2020	6.4	An issue was discovered in Pulse Secure Pulse Connect Secure (PCS) through 2020-04-06. The applet in tncc.jar, executed on macOS, Linux, and Solaris clients when a Host Checker policy is enforced, accepts an arbitrary SSL certificate. **CVE ID : CVE-2020-11580**	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44426	O-ORA-SOLA-270420/318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-04-2020	9.3	An issue was discovered in Pulse Secure Pulse Connect Secure (PCS) through 2020-04-06. The applet in tncc.jar, executed on macOS, Linux, and Solaris clients when a Host Checker policy is enforced, allows a man-in-the-middle attacker to perform OS command injection attacks (against a client) via shell metacharacters to the doCustomRemediateInstructions method, because Runtime.getRuntime().exec() is used. **CVE ID : CVE-2020-11581**	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44426	O-ORA-SOLA-270420/319
Improper Restriction of Excessive Authentication Attempts	06-04-2020	3.3	An issue was discovered in Pulse Secure Pulse Connect Secure (PCS) through 2020-04-06. The applet in tncc.jar, executed on macOS, Linux, and Solaris clients when a Host Checker policy is enforced, launches a TCP server that accepts local connections on a random port. This can be reached by local HTTP clients, because up to 25 invalid lines are ignored, and because DNS rebinding can occur. (This server accepts, for example, a setcookie command that	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44426	O-ORA-SOLA-270420/320

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			might be relevant to CVE-2020-11581 exploitation.) **CVE ID : CVE-2020-11582**		
Paloaltonetworks					
pan-os					
Insufficiently Protected Credentials	08-04-2020	1.9	TechSupport files generated on Palo Alto Networks VM Series firewalls for Microsoft Azure platform configured with high availability (HA) inadvertently collect Azure dashboard service account credentials. These credentials are equivalent to the credentials associated with the Contributor role in Azure. A user with the credentials will be able to manage all the Azure resources in the subscription except for granting access to other resources. These credentials do not allow login access to the VMs themselves. This issue affects VM Series Plugin versions before 1.0.9 for PAN-OS 9.0. This issue does not affect VM Series in non-HA configurations or on other cloud platforms. It does not affect hardware firewall appliances. Since	N/A	O-PAL-PAN--270420/321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			becoming aware of the issue, Palo Alto Networks has safely deleted all the tech support files with the credentials. We now filter and remove these credentials from all TechSupport files sent to us. The TechSupport files uploaded to Palo Alto Networks systems were only accessible by authorized personnel with valid Palo Alto Networks credentials. We do not have any evidence of malicious access or use of these credentials. **CVE ID : CVE-2020-1978**		
Out-of-bounds Write	08-04-2020	9	A stack-based buffer overflow vulnerability in the management server component of PAN-OS allows an authenticated user to upload a corrupted PAN-OS configuration and potentially execute code with root privileges. This issue affects Palo Alto Networks PAN-OS 8.1 versions before 8.1.13; 9.0 versions before 9.0.7. This issue does not affect PAN-OS 7.1. **CVE ID : CVE-2020-1990**	N/A	O-PAL-PAN--270420/322
Use of Externally-Controlled Format String	08-04-2020	9.3	A format string vulnerability in the Varrcvr daemon of PAN-OS on PA-7000 Series	N/A	O-PAL-PAN--270420/323

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			devices with a Log Forwarding Card (LFC) allows remote attackers to crash the daemon creating a denial of service condition or potentially execute code with root privileges. This issue affects Palo Alto Networks PAN-OS 9.0 versions before 9.0.7; PAN-OS 9.1 versions before 9.1.2 on PA-7000 Series devices with an LFC installed and configured. This issue requires WildFire services to be configured and enabled. This issue does not affect PAN-OS 8.1 and earlier releases. This issue does not affect any other PA Series firewalls. **CVE ID : CVE-2020-1992**		
plathome					
easyblocks_ipv6_firmware					
Cross-Site Request Forgery (CSRF)	08-04-2020	6.8	Cross-site request forgery (CSRF) vulnerability in EasyBlocks IPv6 Ver. 2.0.1 and earlier and Enterprise Ver. 2.0.1 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors. **CVE ID : CVE-2020-5549**	N/A	O-PLA-EASY-270420/324
Session	08-04-2020	5.8	Session fixation	N/A	O-PLA-EASY-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Fixation			vulnerability in EasyBlocks IPv6 Ver. 2.0.1 and earlier, and Enterprise Ver. 2.0.1 and earlier allows remote attackers to impersonate a registered user and log in the management console, that may result in information alteration/disclosure via unspecified vectors. **CVE ID : CVE-2020-5550**		270420/325
easyblocks_ipv6_enterprise_firmware					
Cross-Site Request Forgery (CSRF)	08-04-2020	6.8	Cross-site request forgery (CSRF) vulnerability in EasyBlocks IPv6 Ver. 2.0.1 and earlier and Enterprise Ver. 2.0.1 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors. **CVE ID : CVE-2020-5549**	N/A	O-PLA-EASY-270420/326
Session Fixation	08-04-2020	5.8	Session fixation vulnerability in EasyBlocks IPv6 Ver. 2.0.1 and earlier, and Enterprise Ver. 2.0.1 and earlier allows remote attackers to impersonate a registered user and log in the management console, that may result in information alteration/disclosure via unspecified vectors. **CVE ID : CVE-2020-5550**	N/A	O-PLA-EASY-270420/327

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Redhat					
virtualization					
Uncontrolled Resource Consumption	13-04-2020	5	A flaw was found in libssh versions before 0.8.9 and before 0.9.4 in the way it handled AES-CTR (or DES ciphers if enabled) ciphers. The server or client could crash when the connection hasn't been fully initialized and the system tries to cleanup the ciphers when closing the connection. The biggest threat from this vulnerability is system availability. **CVE ID : CVE-2020-1730**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1730	O-RED-VIRT-270420/328
enterprise_linux					
Uncontrolled Resource Consumption	13-04-2020	5	A flaw was found in libssh versions before 0.8.9 and before 0.9.4 in the way it handled AES-CTR (or DES ciphers if enabled) ciphers. The server or client could crash when the connection hasn't been fully initialized and the system tries to cleanup the ciphers when closing the connection. The biggest threat from this vulnerability is system availability. **CVE ID : CVE-2020-1730**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1730	O-RED-ENTE-270420/329
Information Exposure	08-04-2020	2.3	A flaw was discovered in the way that the KVM hypervisor handled instruction emulation for	N/A	O-RED-ENTE-270420/330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an L2 guest when nested virtualisation is enabled. Under some circumstances, an L2 guest may trick the L0 guest into accessing sensitive L1 resources that should be inaccessible to the L2 guest. **CVE ID : CVE-2020-2732**		
ST					
stm32f1_firmware					
Information Exposure	06-04-2020	5	STMicroelectronics STM32F1 devices have Incorrect Access Control. **CVE ID : CVE-2020-8004**	N/A	O-ST-STM3-270420/331
stormshield					
sn310_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	13-04-2020	5.8	Stormshield Network Security 310 3.7.10 devices have an auth/lang.html?rurl= Open Redirect vulnerability on the captive portal. For example, the attacker can use rurl=//example.com instead of rurl=https://example.com in the query string. **CVE ID : CVE-2020-8430**	https://advisories.stormshield.eu/2020-001/	O-STO-SN31-270420/332
Suse					
linux_enterprise_desktop					
Concurrent Execution using Shared	02-04-2020	4.4	A Race Condition Enabling Link Following vulnerability in the	https://bugzilla.suse.com/show_bu	O-SUS-LINU-270420/333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			packaging of texlive-filesystem of SUSE Linux Enterprise Module for Desktop Applications 15-SP1, SUSE Linux Enterprise Software Development Kit 12-SP4, SUSE Linux Enterprise Software Development Kit 12-SP5; openSUSE Leap 15.1 allows local users to corrupt files or potentially escalate privileges. This issue affects: SUSE Linux Enterprise Module for Desktop Applications 15-SP1 texlive-filesystem versions prior to 2017.135-9.5.1. SUSE Linux Enterprise Software Development Kit 12-SP4 texlive-filesystem versions prior to 2013.74-16.5.1. SUSE Linux Enterprise Software Development Kit 12-SP5 texlive-filesystem versions prior to 2013.74-16.5.1. openSUSE Leap 15.1 texlive-filesystem versions prior to 2017.135-lp151.8.3.1. **CVE ID : CVE-2020-8016**	g.cgi?id=1159740	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race	02-04-2020	3.3	A Race Condition Enabling Link Following vulnerability in the cron job shipped with texlive-filesystem of SUSE Linux Enterprise Module for Desktop Applications 15-SP1, SUSE Linux	https://bugzilla.suse.com/show_bug.cgi?id=1158910	O-SUS-LINU-270420/334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Condition')			Enterprise Software Development Kit 12-SP4, SUSE Linux Enterprise Software Development Kit 12-SP5; openSUSE Leap 15.1 allows local users in group mktex to delete arbitrary files on the system This issue affects: SUSE Linux Enterprise Module for Desktop Applications 15-SP1 texlive-filesystem versions prior to 2017.135-9.5.1. SUSE Linux Enterprise Software Development Kit 12-SP4 texlive-filesystem versions prior to 2013.74-16.5.1. SUSE Linux Enterprise Software Development Kit 12-SP5 texlive-filesystem versions prior to 2013.74-16.5.1. openSUSE Leap 15.1 texlive-filesystem versions prior to 2017.135-lp151.8.3.1. **CVE ID : CVE-2020-8017**		
linux_enterprise_software_development_kit					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-04-2020	4.4	A Race Condition Enabling Link Following vulnerability in the packaging of texlive-filesystem of SUSE Linux Enterprise Module for Desktop Applications 15-SP1, SUSE Linux Enterprise Software Development Kit 12-SP4,	https://bugzilla.suse.com/show_bug.cgi?id=1159740	O-SUS-LINU-270420/335

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SUSE Linux Enterprise Software Development Kit 12-SP5; openSUSE Leap 15.1 allows local users to corrupt files or potentially escalate privileges. This issue affects: SUSE Linux Enterprise Module for Desktop Applications 15-SP1 texlive-filesystem versions prior to 2017.135-9.5.1. SUSE Linux Enterprise Software Development Kit 12-SP4 texlive-filesystem versions prior to 2013.74-16.5.1. SUSE Linux Enterprise Software Development Kit 12-SP5 texlive-filesystem versions prior to 2013.74-16.5.1. openSUSE Leap 15.1 texlive-filesystem versions prior to 2017.135-lp151.8.3.1. **CVE ID : CVE-2020-8016**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-04-2020	3.3	A Race Condition Enabling Link Following vulnerability in the cron job shipped with texlive-filesystem of SUSE Linux Enterprise Module for Desktop Applications 15-SP1, SUSE Linux Enterprise Software Development Kit 12-SP4, SUSE Linux Enterprise Software Development Kit 12-SP5; openSUSE Leap 15.1 allows local users in group mktex to delete	https://bugzilla.suse.com/show_bug.cgi?id=1158910	O-SUS-LINU-270420/336

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary files on the system This issue affects: SUSE Linux Enterprise Module for Desktop Applications 15-SP1 texlive-filesystem versions prior to 2017.135-9.5.1. SUSE Linux Enterprise Software Development Kit 12-SP4 texlive-filesystem versions prior to 2013.74-16.5.1. SUSE Linux Enterprise Software Development Kit 12-SP5 texlive-filesystem versions prior to 2013.74-16.5.1. openSUSE Leap 15.1 texlive-filesystem versions prior to 2017.135-lp151.8.3.1. **CVE ID : CVE-2020-8017**		
Technicolor					
tc7337_firmware					
Insufficiently Protected Credentials	01-04-2020	5	An issue was discovered on Technicolor TC7337 8.89.17 devices. An attacker can discover admin credentials in the backup file, aka backupsettings.conf. **CVE ID : CVE-2020-11449**	N/A	O-TEC-TC73-270420/337
Tp-link					
tl-wr841n_firmware					
Buffer Copy without Checking Size of Input	02-04-2020	9	A buffer overflow in the httpd daemon on TP-Link TL-WR841N V10 (firmware version 3.16.9)	N/A	O-TP--TL-W-270420/338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			devices allows an authenticated remote attacker to execute arbitrary code via a GET request to the page for the configuration of the Wi-Fi network. **CVE ID : CVE-2020-8423**		
nc450_firmware					
NULL Pointer Dereference	01-04-2020	5	TP-Link NC200 through 2.1.8_Build_171109, NC210 through 1.0.9_Build_171214, NC220 through 1.3.0_Build_180105, NC230 through 1.3.0_Build_171205, NC250 through 1.3.0_Build_171205, NC260 through 1.5.1_Build_190805, and NC450 through 1.5.0_Build_181022 devices allow a remote NULL Pointer Dereference. **CVE ID : CVE-2020-10231**	N/A	O-TP--NC45-270420/339
Improper Authentication	01-04-2020	5	TP-Link cloud cameras through 2020-02-09 allow remote attackers to bypass authentication and obtain sensitive information via vectors involving a Wi-Fi session with GPS enabled, aka CNVD-2020-04855. **CVE ID : CVE-2020-11445**	N/A	O-TP--NC45-270420/340

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
nc260_firmware					
NULL Pointer Dereference	01-04-2020	5	TP-Link NC200 through 2.1.8_Build_171109, NC210 through 1.0.9_Build_171214, NC220 through 1.3.0_Build_180105, NC230 through 1.3.0_Build_171205, NC250 through 1.3.0_Build_171205, NC260 through 1.5.1_Build_190805, and NC450 through 1.5.0_Build_181022 devices allow a remote NULL Pointer Dereference. **CVE ID : CVE-2020-10231**	N/A	O-TP--NC26-270420/341
Improper Authentication	01-04-2020	5	TP-Link cloud cameras through 2020-02-09 allow remote attackers to bypass authentication and obtain sensitive information via vectors involving a Wi-Fi session with GPS enabled, aka CNVD-2020-04855. **CVE ID : CVE-2020-11445**	N/A	O-TP--NC26-270420/342
nc250_firmware					
NULL Pointer Dereference	01-04-2020	5	TP-Link NC200 through 2.1.8_Build_171109, NC210 through 1.0.9_Build_171214, NC220 through 1.3.0_Build_180105, NC230 through	N/A	O-TP--NC25-270420/343

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.3.0_Build_171205, NC250 through 1.3.0_Build_171205, NC260 through 1.5.1_Build_190805, and NC450 through 1.5.0_Build_181022 devices allow a remote NULL Pointer Dereference. **CVE ID : CVE-2020-10231**		
Improper Authentication	01-04-2020	5	TP-Link cloud cameras through 2020-02-09 allow remote attackers to bypass authentication and obtain sensitive information via vectors involving a Wi-Fi session with GPS enabled, aka CNVD-2020-04855. **CVE ID : CVE-2020-11445**	N/A	O-TP--NC25-270420/344
nc230_firmware					
NULL Pointer Dereference	01-04-2020	5	TP-Link NC200 through 2.1.8_Build_171109, NC210 through 1.0.9_Build_171214, NC220 through 1.3.0_Build_180105, NC230 through 1.3.0_Build_171205, NC250 through 1.3.0_Build_171205, NC260 through 1.5.1_Build_190805, and NC450 through 1.5.0_Build_181022 devices allow a remote NULL Pointer	N/A	O-TP--NC23-270420/345

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Dereference. **CVE ID : CVE-2020-10231**		
Improper Authentication	01-04-2020	5	TP-Link cloud cameras through 2020-02-09 allow remote attackers to bypass authentication and obtain sensitive information via vectors involving a Wi-Fi session with GPS enabled, aka CNVD-2020-04855. **CVE ID : CVE-2020-11445**	N/A	O-TP--NC23-270420/346
nc220_firmware					
NULL Pointer Dereference	01-04-2020	5	TP-Link NC200 through 2.1.8_Build_171109, NC210 through 1.0.9_Build_171214, NC220 through 1.3.0_Build_180105, NC230 through 1.3.0_Build_171205, NC250 through 1.3.0_Build_171205, NC260 through 1.5.1_Build_190805, and NC450 through 1.5.0_Build_181022 devices allow a remote NULL Pointer Dereference. **CVE ID : CVE-2020-10231**	N/A	O-TP--NC22-270420/347
Improper Authentication	01-04-2020	5	TP-Link cloud cameras through 2020-02-09 allow remote attackers to bypass authentication and obtain sensitive	N/A	O-TP--NC22-270420/348

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information via vectors involving a Wi-Fi session with GPS enabled, aka CNVD-2020-04855. **CVE ID : CVE-2020-11445**		
nc210_firmware					
NULL Pointer Dereference	01-04-2020	5	TP-Link NC200 through 2.1.8_Build_171109, NC210 through 1.0.9_Build_171214, NC220 through 1.3.0_Build_180105, NC230 through 1.3.0_Build_171205, NC250 through 1.3.0_Build_171205, NC260 through 1.5.1_Build_190805, and NC450 through 1.5.0_Build_181022 devices allow a remote NULL Pointer Dereference. **CVE ID : CVE-2020-10231**	N/A	O-TP--NC21-270420/349
Improper Authentication	01-04-2020	5	TP-Link cloud cameras through 2020-02-09 allow remote attackers to bypass authentication and obtain sensitive information via vectors involving a Wi-Fi session with GPS enabled, aka CNVD-2020-04855. **CVE ID : CVE-2020-11445**	N/A	O-TP--NC21-270420/350
nc200_firmware					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	01-04-2020	5	TP-Link NC200 through 2.1.8_Build_171109, NC210 through 1.0.9_Build_171214, NC220 through 1.3.0_Build_180105, NC230 through 1.3.0_Build_171205, NC250 through 1.3.0_Build_171205, NC260 through 1.5.1_Build_190805, and NC450 through 1.5.0_Build_181022 devices allow a remote NULL Pointer Dereference. **CVE ID : CVE-2020-10231**	N/A	O-TP--NC20-270420/351
Improper Authentication	01-04-2020	5	TP-Link cloud cameras through 2020-02-09 allow remote attackers to bypass authentication and obtain sensitive information via vectors involving a Wi-Fi session with GPS enabled, aka CNVD-2020-04855. **CVE ID : CVE-2020-11445**	N/A	O-TP--NC20-270420/352
kc300s2_firmware					
Improper Authentication	01-04-2020	5	TP-Link cloud cameras through 2020-02-09 allow remote attackers to bypass authentication and obtain sensitive information via vectors involving a Wi-Fi session with GPS enabled, aka	N/A	O-TP--KC30-270420/353

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CNVD-2020-04855. **CVE ID : CVE-2020-11445**		
kc310s2_firmware					
Improper Authentication	01-04-2020	5	TP-Link cloud cameras through 2020-02-09 allow remote attackers to bypass authentication and obtain sensitive information via vectors involving a Wi-Fi session with GPS enabled, aka CNVD-2020-04855. **CVE ID : CVE-2020-11445**	N/A	O-TP--KC31-270420/354
kc200_firmware					
Improper Authentication	01-04-2020	5	TP-Link cloud cameras through 2020-02-09 allow remote attackers to bypass authentication and obtain sensitive information via vectors involving a Wi-Fi session with GPS enabled, aka CNVD-2020-04855. **CVE ID : CVE-2020-11445**	N/A	O-TP--KC20-270420/355
tapo_c200_firmware					
Improper Authentication	01-04-2020	5	TP-Link cloud cameras through 2020-02-09 allow remote attackers to bypass authentication and obtain sensitive information via vectors involving a Wi-Fi session with GPS enabled, aka CNVD-2020-04855. **CVE ID : CVE-2020-**	N/A	O-TP--TAPO-270420/356

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			11445		
tapo_c100_firmware					
Improper Authentication	01-04-2020	5	TP-Link cloud cameras through 2020-02-09 allow remote attackers to bypass authentication and obtain sensitive information via vectors involving a Wi-Fi session with GPS enabled, aka CNVD-2020-04855. **CVE ID : CVE-2020-11445**	N/A	O-TP--TAPO-270420/357
tl-sc3430_firmware					
Improper Authentication	01-04-2020	5	TP-Link cloud cameras through 2020-02-09 allow remote attackers to bypass authentication and obtain sensitive information via vectors involving a Wi-Fi session with GPS enabled, aka CNVD-2020-04855. **CVE ID : CVE-2020-11445**	N/A	O-TP--TL-S-270420/358
tl-sc3430n_firmware					
Improper Authentication	01-04-2020	5	TP-Link cloud cameras through 2020-02-09 allow remote attackers to bypass authentication and obtain sensitive information via vectors involving a Wi-Fi session with GPS enabled, aka CNVD-2020-04855. **CVE ID : CVE-2020-11445**	N/A	O-TP--TL-S-270420/359
tl-sc4171g_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	01-04-2020	5	TP-Link cloud cameras through 2020-02-09 allow remote attackers to bypass authentication and obtain sensitive information via vectors involving a Wi-Fi session with GPS enabled, aka CNVD-2020-04855. **CVE ID : CVE-2020-11445**	N/A	O-TP--TL-S-270420/360
ui					
cloud_key_gen2					
Improper Authentication	13-04-2020	5	UniFi Cloud Key firmware < 1.1.6 contains a vulnerability that enables an attacker being able to change a device hostname by sending a malicious API request. This affects Cloud Key gen2 and Cloud Key gen2 Plus. **CVE ID : CVE-2020-8148**	N/A	O-UI-CLOU-270420/361
cloud_key_gen2_plus					
Improper Authentication	13-04-2020	5	UniFi Cloud Key firmware < 1.1.6 contains a vulnerability that enables an attacker being able to change a device hostname by sending a malicious API request. This affects Cloud Key gen2 and Cloud Key gen2 Plus. **CVE ID : CVE-2020-8148**	N/A	O-UI-CLOU-270420/362
Yamaha					
rtx830_firmware					
N/A	01-04-2020	7.8	Yamaha LTE VoIP Router(NVR700W	N/A	O-YAM-RTX8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware Rev.15.00.15 and earlier), Yamaha Gigabit VoIP Router(NVR510 firmware Rev.15.01.14 and earlier), Yamaha Gigabit VPN Router(RTX810 firmware Rev.11.01.33 and earlier, RTX830 firmware Rev.15.02.09 and earlier, RTX1200 firmware Rev.10.01.76 and earlier, RTX1210 firmware Rev.14.01.33 and earlier, RTX3500 firmware Rev.14.00.26 and earlier, and RTX5000 firmware Rev.14.00.26 and earlier), Yamaha Broadband VoIP Router(NVR500 firmware Rev.11.00.38 and earlier), and Yamaha Firewall(FWX120 firmware Rev.11.03.27 and earlier) allow remote attackers to cause a denial of service via unspecified vectors. **CVE ID : CVE-2020-5548**		270420/363
nvr510_firmware					
N/A	01-04-2020	7.8	Yamaha LTE VoIP Router(NVR700W firmware Rev.15.00.15 and earlier), Yamaha Gigabit VoIP Router(NVR510 firmware Rev.15.01.14 and earlier), Yamaha Gigabit VPN Router(RTX810 firmware Rev.11.01.33 and earlier,	N/A	O-YAM-NVR5-270420/364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			RTX830 firmware Rev.15.02.09 and earlier, RTX1200 firmware Rev.10.01.76 and earlier, RTX1210 firmware Rev.14.01.33 and earlier, RTX3500 firmware Rev.14.00.26 and earlier, and RTX5000 firmware Rev.14.00.26 and earlier), Yamaha Broadband VoIP Router(NVR500 firmware Rev.11.00.38 and earlier), and Yamaha Firewall(FWX120 firmware Rev.11.03.27 and earlier) allow remote attackers to cause a denial of service via unspecified vectors. **CVE ID : CVE-2020-5548**		
nvr700w_firmware					
N/A	01-04-2020	7.8	Yamaha LTE VoIP Router(NVR700W firmware Rev.15.00.15 and earlier), Yamaha Gigabit VoIP Router(NVR510 firmware Rev.15.01.14 and earlier), Yamaha Gigabit VPN Router(RTX810 firmware Rev.11.01.33 and earlier, RTX830 firmware Rev.15.02.09 and earlier, RTX1200 firmware Rev.10.01.76 and earlier, RTX1210 firmware Rev.14.01.33 and earlier, RTX3500 firmware Rev.14.00.26 and earlier,	N/A	O-YAM-NVR7-270420/365

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and RTX5000 firmware Rev.14.00.26 and earlier), Yamaha Broadband VoIP Router(NVR500 firmware Rev.11.00.38 and earlier), and Yamaha Firewall(FWX120 firmware Rev.11.03.27 and earlier) allow remote attackers to cause a denial of service via unspecified vectors. **CVE ID : CVE-2020-5548**		
rtx1210_firmware					
N/A	01-04-2020	7.8	Yamaha LTE VoIP Router(NVR700W firmware Rev.15.00.15 and earlier), Yamaha Gigabit VoIP Router(NVR510 firmware Rev.15.01.14 and earlier), Yamaha Gigabit VPN Router(RTX810 firmware Rev.11.01.33 and earlier, RTX830 firmware Rev.15.02.09 and earlier, RTX1200 firmware Rev.10.01.76 and earlier, RTX1210 firmware Rev.14.01.33 and earlier, RTX3500 firmware Rev.14.00.26 and earlier, and RTX5000 firmware Rev.14.00.26 and earlier), Yamaha Broadband VoIP Router(NVR500 firmware Rev.11.00.38 and earlier), and Yamaha Firewall(FWX120 firmware Rev.11.03.27	N/A	O-YAM-RTX1-270420/366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and earlier) allow remote attackers to cause a denial of service via unspecified vectors. **CVE ID : CVE-2020-5548**		
rtx5000_firmware					
N/A	01-04-2020	7.8	Yamaha LTE VoIP Router(NVR700W firmware Rev.15.00.15 and earlier), Yamaha Gigabit VoIP Router(NVR510 firmware Rev.15.01.14 and earlier), Yamaha Gigabit VPN Router(RTX810 firmware Rev.11.01.33 and earlier, RTX830 firmware Rev.15.02.09 and earlier, RTX1200 firmware Rev.10.01.76 and earlier, RTX1210 firmware Rev.14.01.33 and earlier, RTX3500 firmware Rev.14.00.26 and earlier, and RTX5000 firmware Rev.14.00.26 and earlier), Yamaha Broadband VoIP Router(NVR500 firmware Rev.11.00.38 and earlier), and Yamaha Firewall(FWX120 firmware Rev.11.03.27 and earlier) allow remote attackers to cause a denial of service via unspecified vectors. **CVE ID : CVE-2020-5548**	N/A	O-YAM-RTX5-270420/367
rtx3500_firmware					
N/A	01-04-2020	7.8	Yamaha LTE VoIP	N/A	O-YAM-RTX3-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Router(NVR700W firmware Rev.15.00.15 and earlier), Yamaha Gigabit VoIP Router(NVR510 firmware Rev.15.01.14 and earlier), Yamaha Gigabit VPN Router(RTX810 firmware Rev.11.01.33 and earlier, RTX830 firmware Rev.15.02.09 and earlier, RTX1200 firmware Rev.10.01.76 and earlier, RTX1210 firmware Rev.14.01.33 and earlier, RTX3500 firmware Rev.14.00.26 and earlier, and RTX5000 firmware Rev.14.00.26 and earlier), Yamaha Broadband VoIP Router(NVR500 firmware Rev.11.00.38 and earlier), and Yamaha Firewall(FWX120 firmware Rev.11.03.27 and earlier) allow remote attackers to cause a denial of service via unspecified vectors. **CVE ID : CVE-2020-5548**		270420/368
fwx120_firmware					
N/A	01-04-2020	7.8	Yamaha LTE VoIP Router(NVR700W firmware Rev.15.00.15 and earlier), Yamaha Gigabit VoIP Router(NVR510 firmware Rev.15.01.14 and earlier), Yamaha Gigabit VPN Router(RTX810 firmware	N/A	O-YAM-FWX1-270420/369

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rev.11.01.33 and earlier, RTX830 firmware Rev.15.02.09 and earlier, RTX1200 firmware Rev.10.01.76 and earlier, RTX1210 firmware Rev.14.01.33 and earlier, RTX3500 firmware Rev.14.00.26 and earlier, and RTX5000 firmware Rev.14.00.26 and earlier), Yamaha Broadband VoIP Router(NVR500 firmware Rev.11.00.38 and earlier), and Yamaha Firewall(FWX120 firmware Rev.11.03.27 and earlier) allow remote attackers to cause a denial of service via unspecified vectors. **CVE ID : CVE-2020-5548**		
rtx810_firmware					
N/A	01-04-2020	7.8	Yamaha LTE VoIP Router(NVR700W firmware Rev.15.00.15 and earlier), Yamaha Gigabit VoIP Router(NVR510 firmware Rev.15.01.14 and earlier), Yamaha Gigabit VPN Router(RTX810 firmware Rev.11.01.33 and earlier, RTX830 firmware Rev.15.02.09 and earlier, RTX1200 firmware Rev.10.01.76 and earlier, RTX1210 firmware Rev.14.01.33 and earlier, RTX3500 firmware	N/A	O-YAM-RTX8-270420/370

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rev.14.00.26 and earlier, and RTX5000 firmware Rev.14.00.26 and earlier), Yamaha Broadband VoIP Router(NVR500 firmware Rev.11.00.38 and earlier), and Yamaha Firewall(FWX120 firmware Rev.11.03.27 and earlier) allow remote attackers to cause a denial of service via unspecified vectors. **CVE ID : CVE-2020-5548**		
nvr500_firmware					
N/A	01-04-2020	7.8	Yamaha LTE VoIP Router(NVR700W firmware Rev.15.00.15 and earlier), Yamaha Gigabit VoIP Router(NVR510 firmware Rev.15.01.14 and earlier), Yamaha Gigabit VPN Router(RTX810 firmware Rev.11.01.33 and earlier, RTX830 firmware Rev.15.02.09 and earlier, RTX1200 firmware Rev.10.01.76 and earlier, RTX1210 firmware Rev.14.01.33 and earlier, RTX3500 firmware Rev.14.00.26 and earlier, and RTX5000 firmware Rev.14.00.26 and earlier), Yamaha Broadband VoIP Router(NVR500 firmware Rev.11.00.38 and earlier), and Yamaha Firewall(FWX120	N/A	O-YAM-NVR5-270420/371

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware Rev.11.03.27 and earlier) allow remote attackers to cause a denial of service via unspecified vectors. **CVE ID : CVE-2020-5548**		
rtx1200_firmware					
N/A	01-04-2020	7.8	Yamaha LTE VoIP Router(NVR700W firmware Rev.15.00.15 and earlier), Yamaha Gigabit VoIP Router(NVR510 firmware Rev.15.01.14 and earlier), Yamaha Gigabit VPN Router(RTX810 firmware Rev.11.01.33 and earlier, RTX830 firmware Rev.15.02.09 and earlier, RTX1200 firmware Rev.10.01.76 and earlier, RTX1210 firmware Rev.14.01.33 and earlier, RTX3500 firmware Rev.14.00.26 and earlier, and RTX5000 firmware Rev.14.00.26 and earlier), Yamaha Broadband VoIP Router(NVR500 firmware Rev.11.00.38 and earlier), and Yamaha Firewall(FWX120 firmware Rev.11.03.27 and earlier) allow remote attackers to cause a denial of service via unspecified vectors. **CVE ID : CVE-2020-5548**	N/A	O-YAM-RTX1-270420/372
Application					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
adb-driver_project					
adb-driver					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-04-2020	7.5	adb-driver through 0.1.8 is vulnerable to Command Injection.It allows execution of arbitrary commands via the command function. **CVE ID : CVE-2020-7636**	N/A	A-ADB-ADB--270420/373
Advantech					
webaccess\/nms					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	09-04-2020	6.5	WebAccess/NMS (versions prior to 3.0.2) does not properly sanitize user input and may allow an attacker to inject system commands remotely. **CVE ID : CVE-2020-10603**	N/A	A-ADV-WEBA-270420/374
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-04-2020	5	There are multiple ways an unauthenticated attacker could perform SQL injection on WebAccess/NMS (versions prior to 3.0.2) to gain access to sensitive information. **CVE ID : CVE-2020-10617**	N/A	A-ADV-WEBA-270420/375
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-04-2020	6.4	An attacker could use a specially crafted URL to delete files outside the WebAccess/NMS's (versions prior to 3.0.2) control. **CVE ID : CVE-2020-**	N/A	A-ADV-WEBA-270420/376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10619		
Unrestricted Upload of File with Dangerous Type	09-04-2020	10	Multiple issues exist that allow files to be uploaded and executed on the WebAccess/NMS (versions prior to 3.0.2). **CVE ID : CVE-2020-10621**	N/A	A-ADV-WEBA-270420/377
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-04-2020	4	Multiple vulnerabilities could allow an attacker with low privileges to perform SQL injection on WebAccess/NMS (versions prior to 3.0.2) to gain access to sensitive information. **CVE ID : CVE-2020-10623**	N/A	A-ADV-WEBA-270420/378
Missing Authentication for Critical Function	09-04-2020	7.5	WebAccess/NMS (versions prior to 3.0.2) allows an unauthenticated remote user to create a new admin account. **CVE ID : CVE-2020-10625**	N/A	A-ADV-WEBA-270420/379
Improper Restriction of XML External Entity Reference ('XXE')	09-04-2020	5	WebAccess/NMS (versions prior to 3.0.2) does not sanitize XML input. Specially crafted XML input could allow an attacker to read sensitive files. **CVE ID : CVE-2020-10629**	N/A	A-ADV-WEBA-270420/380
Improper Limitation of a Pathname to a	09-04-2020	7.5	An attacker could use a specially crafted URL to delete or read files	N/A	A-ADV-WEBA-270420/381

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			outside the WebAccess/NMS's (versions prior to 3.0.2) control. **CVE ID : CVE-2020-10631**		
alienform2_project					
alienform2					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	01-04-2020	10	Jon Hedley AlienForm2 (typically installed as af.cgi or alienform.cgi) 2.0.2 is vulnerable to Remote Command Execution via eval injection, a different issue than CVE-2002-0934. An unauthenticated, remote attacker can exploit this via a series of crafted requests. **CVE ID : CVE-2020-10948**	N/A	A-ALI-ALIE-270420/382
Apache					
cxf					
Information Exposure	01-04-2020	2.9	Apache CXF has the ability to integrate with JMX by registering an InstrumentationManager extension with the CXF bus. If the 'createMBServerConnectorFactory' property of the default InstrumentationManagerImpl is not disabled, then it is vulnerable to a man-in-the-middle (MITM) style attack. An attacker on the same host can	N/A	A-APA-CXF-270420/383

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			connect to the registry and rebind the entry to another server, thus acting as a proxy to the original. They are then able to gain access to all of the information that is sent and received over JMX. **CVE ID : CVE-2020-1954**		
http_server					
URL Redirection to Untrusted Site ('Open Redirect')	02-04-2020	5.8	In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL. **CVE ID : CVE-2020-1927**	https://httpd.apache.org/security/vulnerabilities_24.html, https://security.netapp.com/advisory/ntap-20200413-0002/	A-APA-HTTP-270420/384
Use of Uninitialized Resource	01-04-2020	7.5	In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server. **CVE ID : CVE-2020-1934**	https://httpd.apache.org/security/vulnerabilities_24.html, https://security.netapp.com/advisory/ntap-20200413-0002/	A-APA-HTTP-270420/385
ofbiz					
Improper Neutralization of Input During Web Page	01-04-2020	4.3	Data sent with contentId to /control/stream is not sanitized, allowing XSS attacks in Apache OFBiz	N/A	A-APA-OFBI-270420/386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			16.11.01 to 16.11.07. **CVE ID : CVE-2020-1943**		
sling_cms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-04-2020	4.3	Scripts in Sling CMS before 0.16.0 do not property escape the Sling Selector from URLs when generating navigational elements for the administrative consoles and are vulnerable to reflected XSS attacks. **CVE ID : CVE-2020-1949**	N/A	A-APA-SLIN-270420/387
druid					
Information Exposure	01-04-2020	3.5	When LDAP authentication is enabled in Apache Druid 0.17.0, callers of Druid APIs with a valid set of LDAP credentials can bypass the credentialsValidator.user Search filter barrier that determines if a valid LDAP user is allowed to authenticate with Druid. They are still subject to role-based authorization checks, if configured. Callers of Druid APIs can also retrieve any LDAP attribute values of users that exist on the LDAP server, so long as that information is visible to the Druid server. This information disclosure does not require the caller itself to be a valid LDAP	N/A	A-APA-DRUI-270420/388

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user. **CVE ID : CVE-2020-1958**		
Apachefriends					
xampp					
Improper Privilege Management	02-04-2020	6.8	An issue was discovered in XAMPP before 7.2.29, 7.3.x before 7.3.16 , and 7.4.x before 7.4.4 on Windows. An unprivileged user can change a .exe configuration in xampp-contol.ini for all users (including admins) to enable arbitrary command execution. **CVE ID : CVE-2020-11107**	https://www.apachefriends.org/blog/new_xampp_20200401.html	A-APA-XAMP-270420/389
apiconnect-cli-plugins_project					
apiconnect-cli-plugins					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-04-2020	7.5	apiconnect-cli-plugins through 6.0.1 is vulnerable to Command Injection.It allows execution of arbitrary commands via the pluginUri argument. **CVE ID : CVE-2020-7633**	N/A	A-API-APIC-270420/390
Apple					
icloud					
Always-Incorrect Control Flow Implementation	01-04-2020	4.3	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud	N/A	A-APP-ICLO-270420/391

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for Windows 10.9.3, iCloud for Windows 7.18. A file URL may be incorrectly processed. **CVE ID : CVE-2020-3885**		
N/A	01-04-2020	4.3	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A download's origin may be incorrectly associated. **CVE ID : CVE-2020-3887**	N/A	A-APP-ICLO-270420/392
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-04-2020	2.6	A race condition was addressed with additional validation. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. An application may be able to read restricted memory. **CVE ID : CVE-2020-3894**	N/A	A-APP-ICLO-270420/393
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-04-2020	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for	N/A	A-APP-ICLO-270420/394

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-3895**		
Access of Resource Using Incompatible Type ('Type Confusion')	01-04-2020	9.3	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2020-3897**	N/A	A-APP-ICLO-270420/395
Uncontrolled Resource Consumption	01-04-2020	9.3	A memory consumption issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2020-3899**	N/A	A-APP-ICLO-270420/396
Improper Restriction of Operations	01-04-2020	6.8	A memory corruption issue was addressed with improved memory	N/A	A-APP-ICLO-270420/397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-3900**		
Access of Resource Using Incompatible Type ('Type Confusion')	01-04-2020	6.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-3901**	N/A	A-APP-ICLO-270420/398
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-04-2020	4.3	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously	N/A	A-APP-ICLO-270420/399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted web content may lead to a cross site scripting attack. **CVE ID : CVE-2020-3902**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-04-2020	7.5	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Multiple issues in libxml2. **CVE ID : CVE-2020-3909**	N/A	A-APP-ICLO-270420/400
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-04-2020	7.5	A buffer overflow was addressed with improved size validation. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Multiple issues in libxml2. **CVE ID : CVE-2020-3910**	N/A	A-APP-ICLO-270420/401
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-04-2020	7.5	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2, iTunes for Windows 12.10.5, iCloud for Windows	N/A	A-APP-ICLO-270420/402

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.9.3, iCloud for Windows 7.18. Multiple issues in libxml2. **CVE ID : CVE-2020-3911**		
Use After Free	01-04-2020	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to code execution. **CVE ID : CVE-2020-9783**	N/A	A-APP-ICLO-270420/403
itunes					
Always-Incorrect Control Flow Implementation	01-04-2020	4.3	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A file URL may be incorrectly processed. **CVE ID : CVE-2020-3885**	N/A	A-APP-ITUN-270420/404
N/A	01-04-2020	4.3	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3,	N/A	A-APP-ITUN-270420/405

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			iCloud for Windows 7.18. A download's origin may be incorrectly associated. **CVE ID : CVE-2020-3887**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-04-2020	2.6	A race condition was addressed with additional validation. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. An application may be able to read restricted memory. **CVE ID : CVE-2020-3894**	N/A	A-APP-ITUN-270420/406
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-04-2020	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-3895**	N/A	A-APP-ITUN-270420/407
Access of Resource Using Incompatible Type ('Type Confusion')	01-04-2020	9.3	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4,	N/A	A-APP-ITUN-270420/408

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2020-3897**		
Uncontrolled Resource Consumption	01-04-2020	9.3	A memory consumption issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2020-3899**	N/A	A-APP-ITUN-270420/409
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-04-2020	6.8	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-3900**	N/A	A-APP-ITUN-270420/410

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Access of Resource Using Incompatible Type ('Type Confusion')	01-04-2020	6.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-3901**	N/A	A-APP-ITUN-270420/411
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-04-2020	4.3	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to a cross site scripting attack. **CVE ID : CVE-2020-3902**	N/A	A-APP-ITUN-270420/412
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-04-2020	7.5	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2, iTunes for Windows 12.10.5, iCloud for Windows	N/A	A-APP-ITUN-270420/413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.9.3, iCloud for Windows 7.18. Multiple issues in libxml2. **CVE ID : CVE-2020-3909**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-04-2020	7.5	A buffer overflow was addressed with improved size validation. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Multiple issues in libxml2. **CVE ID : CVE-2020-3910**	N/A	A-APP-ITUN-270420/414
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-04-2020	7.5	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Multiple issues in libxml2. **CVE ID : CVE-2020-3911**	N/A	A-APP-ITUN-270420/415
Use After Free	01-04-2020	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud	N/A	A-APP-ITUN-270420/416

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for Windows 7.18. Processing maliciously crafted web content may lead to code execution. **CVE ID : CVE-2020-9783**		
safari					
Always-Incorrect Control Flow Implementation	01-04-2020	4.3	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A file URL may be incorrectly processed. **CVE ID : CVE-2020-3885**	N/A	A-APP-SAFA-270420/417
N/A	01-04-2020	4.3	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A download's origin may be incorrectly associated. **CVE ID : CVE-2020-3887**	N/A	A-APP-SAFA-270420/418
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	01-04-2020	2.6	A race condition was addressed with additional validation. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18.	N/A	A-APP-SAFA-270420/419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			An application may be able to read restricted memory. **CVE ID : CVE-2020-3894**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-04-2020	9.3	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-3895**	N/A	A-APP-SAFA-270420/420
Access of Resource Using Incompatible Type ('Type Confusion')	01-04-2020	9.3	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2020-3897**	N/A	A-APP-SAFA-270420/421
Uncontrolled Resource Consumption	01-04-2020	9.3	A memory consumption issue was addressed with improved memory handling. This issue is	N/A	A-APP-SAFA-270420/422

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A remote attacker may be able to cause arbitrary code execution. **CVE ID : CVE-2020-3899**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-04-2020	6.8	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2020-3900**	N/A	A-APP-SAFA-270420/423
Access of Resource Using Incompatible Type ('Type Confusion')	01-04-2020	6.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to arbitrary code	N/A	A-APP-SAFA-270420/424

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2020-3901**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-04-2020	4.3	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to a cross site scripting attack. **CVE ID : CVE-2020-3902**	N/A	A-APP-SAFA-270420/425
Use After Free	01-04-2020	6.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to code execution. **CVE ID : CVE-2020-9783**	N/A	A-APP-SAFA-270420/426
N/A	01-04-2020	4.3	A logic issue was addressed with improved restrictions. This issue is fixed in Safari 13.1. A malicious iframe may use another website's download settings. **CVE ID : CVE-2020-9784**	N/A	A-APP-SAFA-270420/427

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mac_os_x					
N/A	01-04-2020	6.8	This issue was addressed with improved checks. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. An application may be able to use arbitrary entitlements. **CVE ID : CVE-2020-3883**	N/A	A-APP-MAC_-270420/428
auth0					
login_by_auth0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-04-2020	4.3	The Login by Auth0 plugin before 4.0.0 for WordPress allows stored XSS on multiple pages, a different issue than CVE-2020-5392. **CVE ID : CVE-2020-6753**	https://auth0.com/docs/security/bulletins/2020-03-31_wpauth0, https://github.com/auth0/wp-auth0/security/advisories/GHSA-59vf-cgfw-6h6v	A-AUT-LOGI-270420/429
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	01-04-2020	7.5	An issue was discovered in the Login by Auth0 plugin before 4.0.0 for WordPress. It has numerous fields that can contain data that is pulled from different sources. One issue with this is that the data isn't sanitized, and no input validation is performed, before the	https://auth0.com/docs/security/bulletins/2020-03-31_wpauth0, https://github.com/auth0/wp-auth0/secu	A-AUT-LOGI-270420/430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exporting of the user data. This can lead to (at least) CSV injection if a crafted Excel document is uploaded. **CVE ID : CVE-2020-7947**	rity/advisories/GHSA-59vf-cgfw-6h6v	
N/A	01-04-2020	6.5	An issue was discovered in the Login by Auth0 plugin before 4.0.0 for WordPress. A user can perform an insecure direct object reference. **CVE ID : CVE-2020-7948**	https://auth0.com/docs/security/bulletins/2020-03-31_wpauth0, https://github.com/auth0/wp-auth0/security/advisories/GHSA-59vf-cgfw-6h6v	A-AUT-LOGI-270420/431
auth0.js					
Insufficiently Protected Credentials	09-04-2020	4	auth0.js (NPM package auth0-js) greater than version 8.0.0 and before version 9.12.3 has a vulnerability. In the case of an (authentication) error, the error object returned by the library contains the original request of the user, which may include the plaintext password the user entered. If the error object is exposed or logged without modification, the application risks password exposure. This	https://github.com/auth0/auth0.js/security/advisories/GHSA-prfq-f66g-43mp	A-AUT-AUTH-270420/432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is fixed in version 9.12.3 **CVE ID : CVE-2020-5263**		
wp-auth0					
Cross-Site Request Forgery (CSRF)	01-04-2020	6.8	Cross-site request forgery (CSRF) vulnerabilities exist in the Auth0 plugin before 4.0.0 for WordPress via the domain field. **CVE ID : CVE-2020-5391**	https://auth0.com/docs/security/bulletins/2020-03-31_wpauth0, https://github.com/auth0/wp-auth0/security/advisories/GHSA-59vf-cgfw-6h6v	A-AUT-WP-A-270420/433
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-04-2020	4.3	A stored cross-site scripting (XSS) vulnerability exists in the Auth0 plugin before 4.0.0 for WordPress via the settings page. **CVE ID : CVE-2020-5392**	https://auth0.com/docs/security/bulletins/2020-03-31_wpauth0, https://github.com/auth0/wp-auth0/security/advisories/GHSA-59vf-cgfw-6h6v	A-AUT-WP-A-270420/434
Avast					
antivirus					
Out-of-bounds Write	01-04-2020	5	An issue was discovered in Avast Antivirus before 20. An Arbitrary Memory Address Overwrite	N/A	A-AVA-ANTI-270420/435

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in the aswAvLog Log Library results in Denial of Service of the Avast Service (AvastSvc.exe). **CVE ID : CVE-2020-10860**		
Improper Input Validation	01-04-2020	6.4	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to achieve Arbitrary File Deletion from Avast Program Path via RPC, when Self Defense is Enabled. **CVE ID : CVE-2020-10861**	N/A	A-AVA-ANTI-270420/436
Improper Privilege Management	01-04-2020	4.6	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to achieve Local Privilege Escalation (LPE) via RPC. **CVE ID : CVE-2020-10862**	N/A	A-AVA-ANTI-270420/437
Improper Input Validation	01-04-2020	5	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to trigger	N/A	A-AVA-ANTI-270420/438

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a shutdown via RPC from a Low Integrity process via TempShutDownMachine. **CVE ID : CVE-2020-10863**		
Improper Input Validation	01-04-2020	5	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to trigger a reboot via RPC from a Low Integrity process. **CVE ID : CVE-2020-10864**	N/A	A-AVA-ANTI-270420/439
Inclusion of Functionality from Untrusted Control Sphere	01-04-2020	5	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to make arbitrary changes to the Components section of the Stats.ini file via RPC from a Low Integrity process. **CVE ID : CVE-2020-10865**	N/A	A-AVA-ANTI-270420/440
Inadequate Encryption Strength	01-04-2020	5	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to enumerate the network	N/A	A-AVA-ANTI-270420/441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interfaces and access points from a Low Integrity process via RPC. **CVE ID : CVE-2020-10866**		
Exposure of Resource to Wrong Sphere	01-04-2020	7.5	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to bypass intended access restrictions on tasks from an untrusted process, when Self Defense is enabled. **CVE ID : CVE-2020-10867**	N/A	A-AVA-ANTI-270420/442
Incorrect Permission Assignment for Critical Resource	01-04-2020	5	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to launch the Repair App RPC call from a Low Integrity process. **CVE ID : CVE-2020-10868**	N/A	A-AVA-ANTI-270420/443
Avira					
free_antivirus					
Improper Control of Generation of Code ('Code Injection')	09-04-2020	7.5	An issue was discovered in Avira Free-Antivirus before 15.0.2004.1825. The Self-Protection feature does not prohibit a write operation from an	https://support.avira.com/hc/en-us/articles/360000109798-Avira-	A-AVI-FREE-270420/444

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			external process. Thus, code injection can be used to turn off this feature. After that, one can construct an event that will modify a file at a specific location, and pass this event to the driver, thereby defeating the anti-virus functionality. **CVE ID : CVE-2020-8961**	Antivirus-for-Windows	
bit2spr_project					
bit2spr					
Out-of-bounds Write	04-04-2020	5	bit2spr 1992-06-07 has a stack-based buffer overflow (129-byte write) in conv_bitmap in bit2spr.c via a long line in a bitmap file. **CVE ID : CVE-2020-11528**	N/A	A-BIT-BIT2-270420/445
Bitdefender					
antimalware_software_development_kit					
Untrusted Search Path	07-04-2020	4.6	Untrusted Search Path vulnerability in Bitdefender High-Level Antimalware SDK for Windows allows an attacker to load third party code from a DLL library in the search path. This issue affects: Bitdefender High-Level Antimalware SDK for Windows versions prior to 3.0.1.204 . **CVE ID : CVE-2020-8096**	https://www.bitdefender.com/support/security-advisories/untrusted-search-path-vulnerability-high-level-antimalware-sdk-windows/	A-BIT-ANTI-270420/446

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
castlerock					
snmpc_online					
Cross-Site Request Forgery (CSRF)	09-04-2020	6.8	An issue was discovered in Castle Rock SNMPc Online 12.10.10 before 2020-01-28. There is pervasive CSRF. **CVE ID : CVE-2020-11553**	N/A	A-CAS-SNMP-270420/447
Information Exposure	09-04-2020	5	An issue was discovered in Castle Rock SNMPc Online 12.10.10 before 2020-01-28. It allows remote attackers to obtain sensitive information via info.php4. **CVE ID : CVE-2020-11554**	N/A	A-CAS-SNMP-270420/448
Insufficiently Protected Credentials	09-04-2020	5	An issue was discovered in Castle Rock SNMPc Online 12.10.10 before 2020-01-28. It allows remote attackers to obtain sensitive credential information from backup files. **CVE ID : CVE-2020-11555**	N/A	A-CAS-SNMP-270420/449
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-04-2020	3.5	An issue was discovered in Castle Rock SNMPc Online 12.10.10 before 2020-01-28. There are multiple persistent (stored) and reflected XSS vulnerabilities. **CVE ID : CVE-2020-11556**	N/A	A-CAS-SNMP-270420/450
Insufficiently	09-04-2020	5	An issue was discovered	N/A	A-CAS-SNMP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			in Castle Rock SNMPc Online 12.10.10 before 2020-01-28. It includes the username and password values in cleartext within each request's cookie value. **CVE ID : CVE-2020-11557**		270420/451
cipplanner					
cipace					
Improper Restriction of XML External Entity Reference ('XXE')	06-04-2020	7.5	An XXE issue was discovered in CIPPlanner CIPAce 9.1 Build 2019092801. An unauthenticated attacker can make an API request that contains malicious XML DTD data. **CVE ID : CVE-2020-11586**	N/A	A-CIP-CIPA-270420/452
Information Exposure	06-04-2020	5	An issue was discovered in CIPPlanner CIPAce 9.1 Build 2019092801. An unauthenticated attacker can make an API request and get the content of ETL Processes running on the server. **CVE ID : CVE-2020-11587**	N/A	A-CIP-CIPA-270420/453
Information Exposure	06-04-2020	5	An issue was discovered in CIPPlanner CIPAce 9.1 Build 2019092801. An unauthenticated attacker can make an HTTP GET request to two files that contain customer data	N/A	A-CIP-CIPA-270420/454

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and application paths. **CVE ID : CVE-2020-11588**		
Information Exposure	06-04-2020	5	An Insecure Direct Object Reference issue was discovered in CIPPlanner CIPAce 9.1 Build 2019092801. An unauthenticated attacker can make a GET request to a certain URL and obtain information that should be provided to authenticated users only. **CVE ID : CVE-2020-11589**	N/A	A-CIP-CIPA-270420/455
Information Exposure	06-04-2020	5	An issue was discovered in CIPPlanner CIPAce 9.1 Build 2019092801. An unauthenticated attacker can make an HTTP GET request to HealthPage.aspx and obtain the internal server name. **CVE ID : CVE-2020-11590**	N/A	A-CIP-CIPA-270420/456
Information Exposure	06-04-2020	5	An issue was discovered in CIPPlanner CIPAce 9.1 Build 2019092801. An unauthenticated attacker can make an API request and obtain the full application path along with the customer name. **CVE ID : CVE-2020-11591**	N/A	A-CIP-CIPA-270420/457
Information	06-04-2020	5	An issue was discovered in CIPPlanner CIPAce 9.1	N/A	A-CIP-CIPA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			Build 2019092801. An unauthenticated attacker can make an API request and get the columns of a specific table within the CIP database. **CVE ID : CVE-2020-11592**		270420/458
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-04-2020	5	An issue was discovered in CIPPlanner CIPAce 9.1 Build 2019092801. An unauthenticated attacker can make an HTTP POST request with injected HTML data that is later leveraged to send emails from a customer trusted email address. **CVE ID : CVE-2020-11593**	N/A	A-CIP-CIPA-270420/459
Information Exposure	06-04-2020	5	An issue was discovered in CIPPlanner CIPAce 9.1 Build 2019092801. An unauthenticated attacker can make an API request that causes a stack error to be shown providing the full file path. **CVE ID : CVE-2020-11594**	N/A	A-CIP-CIPA-270420/460
Information Exposure	06-04-2020	5	An issue was discovered in CIPPlanner CIPAce 9.1 Build 2019092801. An unauthenticated attacker can make an API request and obtain the upload folder path that includes the hostname in a UNC path.	N/A	A-CIP-CIPA-270420/461

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-11595		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-04-2020	5	A Directory Traversal issue was discovered in CIPPlanner CIPAce 9.1 Build 2019092801. An unauthenticated attacker can make HTTP GET requests to a certain URL and obtain information about what files and directories reside on the server. **CVE ID : CVE-2020-11596**	N/A	A-CIP-CIPA-270420/462
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-04-2020	7.5	An issue was discovered in CIPPlanner CIPAce 9.1 Build 2019092801. An unauthenticated attacker can make an HTTP POST request and inject SQL statements in the user context of the db owner. **CVE ID : CVE-2020-11597**	N/A	A-CIP-CIPA-270420/463
Improper Authentication	06-04-2020	7.5	An issue was discovered in CIPPlanner CIPAce 9.1 Build 2019092801. Upload.ashx allows remote attackers to execute arbitrary code by uploading and executing an ASHX file. **CVE ID : CVE-2020-11598**	N/A	A-CIP-CIPA-270420/464
Information Exposure	06-04-2020	5	An issue was discovered in CIPPlanner CIPAce 6.80 Build 2016031401. GetDistributedPOP3	N/A	A-CIP-CIPA-270420/465

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows attackers to obtain the username and password of the SMTP user. **CVE ID : CVE-2020-11599**		
Cisco					
webex_meetings_server					
Improper Input Validation	13-04-2020	3.5	vulnerability within the Multimedia Viewer feature of Cisco Webex Meetings could allow an authenticated, remote attacker to bypass security protections. The vulnerability is due to missing security warning dialog boxes when a room host views shared multimedia files. An authenticated, remote attacker could exploit this vulnerability by using the host role to share files within the Multimedia sharing feature and convincing a former room host to view that file. A warning dialog normally appears cautioning users before the file is displayed; however, the former host would not see that warning dialog, and any shared multimedia would be rendered within the user's browser. The attacker could leverage this behavior to conduct additional attacks by	N/A	A-CIS-WEBE-270420/466

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			including malicious files within a targeted room host's browser window. **CVE ID : CVE-2020-3126**		
clamscan_project					
clamscan					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	07-04-2020	6.8	clamscan through 1.2.0 is vulnerable to Command Injection. It is possible to inject arbitrary commands as part of the `_is_clamav_binary` function located within `Index.js`. It should be noted that this vulnerability requires a pre-requisite that a folder should be created with the same command that will be chained to execute. This lowers the risk of this issue. **CVE ID : CVE-2020-7613**	N/A	A-CLA-CLAM-270420/467
class-transformer_project					
class-transformer					
Improper Input Validation	06-04-2020	5	class-transformer through 0.2.3 is vulnerable to Prototype Pollution. The 'classToPlainFromExist' function could be tricked into adding or modifying properties of 'Object.prototype' using a '__proto__' payload. **CVE ID : CVE-2020-7637**	N/A	A-CLA-CLAS-270420/468
cncf					
argo_continuous_delivery					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	08-04-2020	5	Fixed in v1.5.1, Argo version v1.5.0 was vulnerable to a user-enumeration vulnerability which allowed attackers to determine the usernames of valid (non-SSO) accounts within Argo. **CVE ID : CVE-2020-11576**	N/A	A-CNC-ARGO-270420/469
codeblocks					
code					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-04-2020	4.3	A buffer overflow vulnerability in Code::Blocks 17.12 allows an attacker to execute arbitrary code via a crafted project file. **CVE ID : CVE-2020-10814**	N/A	A-COD-CODE-270420/470
communilink					
clink_office					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-04-2020	4.3	A cross-site scripting (XSS) vulnerability in the index page of the CLink Office 2.0 management console allows remote attackers to inject arbitrary web script or HTML via the lang parameter. **CVE ID : CVE-2020-6171**	N/A	A-COM-CLIN-270420/471
compass-compile_project					
compass-compile					
Improper Neutralization	06-04-2020	7.5	compass-compile through 0.0.1 is vulnerable to	N/A	A-COM-COMP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Special Elements in Output Used by a Downstream Component ('Injection')			Command Injection.It allows execution of arbitrary commands via tha options argument. **CVE ID : CVE-2020-7635**		270420/472
confinit_project					
confinit					
Improper Input Validation	06-04-2020	5	confinit through 0.3.0 is vulnerable to Prototype Pollution.The 'setDeepProperty' function could be tricked into adding or modifying properties of 'Object.prototype' using a '__proto__' payload. **CVE ID : CVE-2020-7638**	N/A	A-CON-CONF-270420/473
contact-form-7-datepicker_project					
contact-form-7-datepicker					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-04-2020	3.5	Stored XSS in the Contact Form 7 Datepicker plugin through 2.6.0 for WordPress allows authenticated attackers with minimal permissions to save arbitrary JavaScript to the plugin's settings via the unprotected wp_ajax_cf7dp_save_settings AJAX action and the ui_theme parameter. If an administrator creates or modifies a contact form, the JavaScript will be executed in their browser, which can then be used to create new administrative	N/A	A-CON-CONT-270420/474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			users or perform other actions using the administrator's session. **CVE ID : CVE-2020-11516**		
cpp-httplib_project					
cpp-httplib					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	12-04-2020	5	cpp-httplib through 0.5.8 does not filter \r\n in parameters passed into the set_redirect and set_header functions, which creates possibilities for CRLF injection and HTTP response splitting in some specific contexts. **CVE ID : CVE-2020-11709**	N/A	A-CPP-CPP--270420/475
cross_domain_local_storage_project					
cross_domain_local_storage					
Improper Input Validation	07-04-2020	6.8	An issue was discovered in xdLocalStorage through 2.0.5. The postData() function in xdLocalStoragePostMessageApi.js specifies the wildcard (*) as the targetOrigin when calling the postMessage() function on the parent object. Therefore any domain can load the application hosting the "magical iframe" and receive the messages that the "magical iframe" sends. **CVE ID : CVE-2020-**	N/A	A-CRO-CROS-270420/476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			11610		
URL Redirection to Untrusted Site ('Open Redirect')	07-04-2020	5.8	An issue was discovered in xdLocalStorage through 2.0.5. The buildMessage() function in xdLocalStorage.js specifies the wildcard (*) as the targetOrigin when calling the postMessage() function on the iframe object. Therefore any domain that is currently loaded within the iframe can receive the messages that the client sends. **CVE ID : CVE-2020-11611**	N/A	A-CRO-CROS-270420/477
ctfd					
rctf					
Session Fixation	01-04-2020	4.3	In RedpwnCTF before version 2.3, there is a session fixation vulnerability in exploitable through the `#token=$ssid` hash when making a request to the `/verify` endpoint. An attacker team could potentially steal flags by, for example, exploiting a stored XSS payload in a CTF challenge so that victim teams who solve the challenge are unknowingly (and against their will) signed into the attacker team's account. Then, the attacker can gain points / value off the backs of the	https://github.com/redpwn/rctf/security/advisories/GHSA-p5fh-2vhw-fvpq	A-CTF-RCTF-270420/478

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			victims. This is patched in version 2.3. **CVE ID : CVE-2020-5290**		
cybersolutions					
cybermail					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-04-2020	4.3	cgi-bin/go in CyberSolutions CyberMail 5 or later allows XSS via the ACTION parameter. **CVE ID : CVE-2020-11734**	N/A	A-CYB-CYBE-270420/479
Dell					
emc_isilon_onefs					
Uncontrolled Resource Consumption	04-04-2020	5	Dell EMC Isilon OneFS versions 8.2.2 and earlier contain a denial of service vulnerability. SmartConnect had an error condition that may be triggered to loop, using CPU and potentially preventing other SmartConnect DNS responses. **CVE ID : CVE-2020-5347**	N/A	A-DEL-EMC_-270420/480
Deskpro					
deskpro					
Improper Privilege Management	01-04-2020	5	An issue was discovered in Deskpro before 2019.8.0. The /api/email_accounts endpoint failed to properly validate a user's privilege, allowing an attacker to retrieve cleartext credentials of all helpdesk email accounts,	N/A	A-DES-DESK-270420/481

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			including incoming and outgoing email credentials. This enables an attacker to get full access to all emails sent or received by the system including password reset emails, making it possible to reset any user's password. **CVE ID : CVE-2020-11463**		
Information Exposure	01-04-2020	4	An issue was discovered in Deskpro before 2019.8.0. The /api/people endpoint failed to properly validate a user's privilege, allowing an attacker to retrieve sensitive information about all users registered on the system. This includes their full name, privilege, email address, phone number, etc. **CVE ID : CVE-2020-11464**	N/A	A-DES-DESK-270420/482
Improper Privilege Management	01-04-2020	6.5	An issue was discovered in Deskpro before 2019.8.0. The /api/apps/* endpoints failed to properly validate a user's privilege, allowing an attacker to control/install helpdesk applications and leak current applications' configurations, including applications used as user sources (used for	N/A	A-DES-DESK-270420/483

CVSS Scoring Scale	0-1	1-2	2-3	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). This enables an attacker to forge valid authentication models that resembles any user on the system. **CVE ID : CVE-2020-11465**		
Information Exposure	01-04-2020	4	An issue was discovered in Deskpro before 2019.8.0. The /api/tickets endpoint failed to properly validate a user's privilege, allowing an attacker to retrieve arbitrary information about all helpdesk tickets stored in database with numerous filters. This leaked sensitive information to unauthorized parties. Additionally, it leaked ticket authentication code, making it possible to make changes to a ticket. **CVE ID : CVE-2020-11466**	N/A	A-DES-DESK-270420/484
Incorrect Permission Assignment for Critical Resource	01-04-2020	6.5	An issue was discovered in Deskpro before 2019.8.0. This product enables administrators to modify the helpdesk interface by editing /portal/api/style/edit-theme-set/template-sources theme templates, and uses TWIG as its template engine. While direct access to self and	N/A	A-DES-DESK-270420/485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			_self variables was not permitted, one could abuse the accessible variables in one's context to reach a native unserialize function via the code parameter. There, on could pass a crafted payload to trigger a set of POP gadgets in order to achieve remote code execution. **CVE ID : CVE-2020-11467**		
diskusage-ng_project					
diskusage-ng					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-04-2020	7.5	diskusage-ng through 0.2.4 is vulnerable to Command Injection.It allows execution of arbitrary commands via the path argument. **CVE ID : CVE-2020-7631**	N/A	A-DIS-DISK-270420/486
dnnsoftware					
dotnetnuke					
Information Exposure	06-04-2020	4	There is an information disclosure issue in DNN (formerly DotNetNuke) 9.5 within the built-in Activity-Feed/Messaging/Userid/Message Center module. A registered user is able to enumerate any file in the Admin File Manager (other than ones contained in a secure folder) by sending	N/A	A-DNN-DOTN-270420/487

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			themselves a message with the file attached, e.g., by using an arbitrary small integer value in the fileIds parameter. **CVE ID : CVE-2020-11585**		
dot_project					
dot					
Improper Input Validation	06-04-2020	5	eivindfjeldstad-dot below 1.0.3 is vulnerable to Prototype Pollution.The function 'set' could be tricked into adding or modifying properties of 'Object.prototype' using a '__proto__' payload. **CVE ID : CVE-2020-7639**	N/A	A-DOT-DOT-270420/488
dropwizard					
dropwizard_validation					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	10-04-2020	9	dropwizard-validation before versions 2.0.3 and 1.3.21 has a remote code execution vulnerability. A server-side template injection was identified in the self-validating feature enabling attackers to inject arbitrary Java EL expressions, leading to Remote Code Execution (RCE) vulnerability. If you are using a self-validating bean an upgrade to Dropwizard 1.3.21/2.0.3 or later is strongly recommended. The changes introduced in Dropwizard 1.3.19 and	https://github.com/dropwizard/dropwizard/security/advisories/GHSA-8jpx-m2wh-2v34	A-DRO-DROP-270420/489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.0.2 for CVE-2020-5245 unfortunately did not fix the underlying issue completely. The issue has been fixed in dropwizard-validation 1.3.21 and 2.0.3 or later. We strongly recommend upgrading to one of these versions. **CVE ID : CVE-2020-11002**		
dungeon_crawl_stone_soup_project					
dungeon_crawl_stone_soup					
Unrestricted Upload of File with Dangerous Type	12-04-2020	7.5	Dungeon Crawl Stone Soup (aka DCSS or crawl) before 0.25 allows remote attackers to execute arbitrary code via Lua bytecode embedded in an uploaded .crawlrc file. **CVE ID : CVE-2020-11722**	N/A	A-DUN-DUNG-270420/490
Eclipse					
che					
Missing Authorization	03-04-2020	4.9	A flaw was found in the Eclipse Che up to version 7.8.x, where it did not properly restrict access to workspace pods. An authenticated user can exploit this flaw to bypass JWT proxy and gain access to the workspace pods of another user. Successful exploitation requires knowledge of the service name and namespace of the target	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10689	A-ECL-CHE-270420/491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			pod. **CVE ID : CVE-2020-10689**		
effect_project					
effect					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	02-04-2020	7.5	effect through 1.0.4 is vulnerable to Command Injection. It allows execution of arbitrary command via the options argument. **CVE ID : CVE-2020-7624**	N/A	A-EFF-EFFE-270420/492
Exim					
exim					
Improper Link Resolution Before File Access ('Link Following')	02-04-2020	7.2	A UNIX Symbolic Link (Symlink) Following vulnerability in the packaging of exim in openSUSE Factory allows local attackers to escalate from user mail to root. This issue affects: openSUSE Factory exim versions prior to 4.93.0.4-3.1. **CVE ID : CVE-2020-8015**	https://bugzilla.suse.com/show_bug.cgi?id=1154183	A-EXI-EXIM-270420/493
express-mock-middleware_project					
express-mock-middleware					
Improper Input Validation	07-04-2020	5	express-mock-middleware through 0.0.6 is vulnerable to Prototype Pollution. Exported functions by the package can be tricked into adding or modifying properties of the `Object.prototype`. Exploitation of this	N/A	A-EXP-EXPR-270420/494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability requires creation of a new directory where an attack code can be placed which will then be exported by `express-mock-middleware`. As such, this is considered to be a low risk. **CVE ID : CVE-2020-7616**		
Facebook					
instagram					
Integer Overflow or Wraparound	09-04-2020	6.8	A large heap overflow could occur in Instagram for Android when attempting to upload an image with specially crafted dimensions. This affects versions prior to 128.0.0.26.128. **CVE ID : CVE-2020-1895**	https://www.facebook.com/security/advisories/cve-2020-1895	A-FAC-INST-270420/495
Fasterxml					
jackson-databind					
Deserialization of Untrusted Data	07-04-2020	6.8	FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.springframework.aop.config.MethodLocatingFactoryBean (aka spring-aop). **CVE ID : CVE-2020-11619**	N/A	A-FAS-JACK-270420/496
Deserialization of Untrusted Data	07-04-2020	6.8	FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the	N/A	A-FAS-JACK-270420/497

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction between serialization gadgets and typing, related to org.apache.commons.jelly.impl.Embedded (aka commons-jelly). **CVE ID : CVE-2020-11620**		
firmware_analysis_and_comparison_tool_project					
firmware_analysis_and_comparison_tool					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-04-2020	4.3	Firmware Analysis and Comparison Tool (FACT) 3 has Stored XSS when updating analysis details via a localhost web request, as demonstrated by mishandling of the tags and version fields in helperFunctions/mongo_task_conversion.py. **CVE ID : CVE-2020-11499**	N/A	A-FIR-FIRM-270420/498
fsa_project					
fsa					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-04-2020	4.6	fsa through 0.5.1 is vulnerable to Command Injection. The first argument of 'execGitCommand()', located within 'lib/rep.js#63' can be controlled by users without any sanitization to inject arbitrary commands. **CVE ID : CVE-2020-7615**	N/A	A-FSA-FSA-270420/499
fujielectric					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
v-server					
Out-of-bounds Write	13-04-2020	6.8	Fuji Electric V-Server Lite all versions prior to 4.0.9.0 contains a heap based buffer overflow. The buffer allocated to read data, when parsing VPR files, is too small. **CVE ID : CVE-2020-10646**	N/A	A-FUJ-V-SE-270420/500
get-git-data_project					
get-git-data					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	02-04-2020	7.5	get-git-data through 1.3.1 is vulnerable to Command Injection. It is possible to inject arbitrary commands as part of the arguments provided to get-git-data. **CVE ID : CVE-2020-7619**	N/A	A-GET-GET--270420/501
getgrav					
grav					
URL Redirection to Untrusted Site ('Open Redirect')	04-04-2020	5.8	Common/Grav.php in Grav before 1.6.23 has an Open Redirect. **CVE ID : CVE-2020-11529**	N/A	A-GET-GRAV-270420/502
git-add-remote_project					
git-add-remote					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	02-04-2020	7.5	git-add-remote through 1.0.0 is vulnerable to Command Injection. It allows execution of arbitrary commands via the name argument. **CVE ID : CVE-2020-7630**	N/A	A-GIT-GIT--270420/503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Gitlab					
gitlab					
Information Exposure	08-04-2020	4	GitLab EE/CE 10.8 to 12.9 is leaking metadata and comments on vulnerabilities to unauthorized users on the vulnerability feedback page. **CVE ID : CVE-2020-10975**	https://about.gitlab.com/releases/2020/03/26/security-release-12-dot-9-dot-1-released/	A-GIT-GITL-270420/504
Information Exposure	08-04-2020	5	GitLab EE/CE 8.17 to 12.9 is vulnerable to information leakage when querying a merge request widget. **CVE ID : CVE-2020-10976**	https://about.gitlab.com/releases/2020/03/26/security-release-12-dot-9-dot-1-released/	A-GIT-GITL-270420/505
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-04-2020	2.1	GitLab EE/CE 8.5 to 12.9 is vulnerable to a an path traversal when moving an issue between projects. **CVE ID : CVE-2020-10977**	https://about.gitlab.com/releases/2020/03/26/security-release-12-dot-9-dot-1-released/	A-GIT-GITL-270420/506
Information Exposure	08-04-2020	5	GitLab EE/CE 8.11 to 12.9 is leaking information on Issues opened in a public project and then moved to a private project through Web-UI and GraphQL API. **CVE ID : CVE-2020-10978**	https://about.gitlab.com/releases/2020/03/26/security-release-12-dot-9-dot-1-released/	A-GIT-GITL-270420/507
Information Exposure	08-04-2020	4	GitLab EE/CE 11.10 to 12.9 is leaking information on restricted CI pipelines metrics to	https://about.gitlab.com/releases/2020/03/	A-GIT-GITL-270420/508

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized users. **CVE ID : CVE-2020-10979**	26/security-release-12-dot-9-dot-1-released/	
Server-Side Request Forgery (SSRF)	08-04-2020	7.5	GitLab EE/CE 8.0.rc1 to 12.9 is vulnerable to a blind SSRF in the FogBugz integration. **CVE ID : CVE-2020-10980**	https://about.gitlab.com/releases/2020/03/26/security-release-12-dot-9-dot-1-released/	A-GIT-GITL-270420/509
Improper Input Validation	08-04-2020	4	GitLab EE/CE 9.0 to 12.9 allows a maintainer to modify other maintainers' pipeline trigger descriptions within the same project. **CVE ID : CVE-2020-10981**	https://about.gitlab.com/releases/2020/03/26/security-release-12-dot-9-dot-1-released/	A-GIT-GITL-270420/510
Gnome					
file-roller					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	13-04-2020	2.1	fr-archive-libarchive.c in GNOME file-roller through 3.36.1 allows Directory Traversal during extraction because it lacks a check of whether a file's parent is a symlink to a directory outside of the intended extraction location. **CVE ID : CVE-2020-11736**	N/A	A-GNO-FILE-270420/511
GNU					
glibc					
Integer Underflow	01-04-2020	7.5	An exploitable signed comparison vulnerability	N/A	A-GNU-GLIB-270420/512

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(Wrap or Wraparound)			exists in the ARMv7 memcpy() implementation of GNU glibc 2.30.9000. Calling memcpy() (on ARMv7 targets that utilize the GNU glibc implementation) with a negative value for the 'num' parameter results in a signed comparison vulnerability. If an attacker underflows the 'num' parameter to memcpy(), this vulnerability could lead to undefined behavior such as writing to out-of-bounds memory and potentially remote code execution. Furthermore, this memcpy() implementation allows for program execution to continue in scenarios where a segmentation fault or crash should have occurred. The dangers occur in that subsequent execution and iterations of this code will be executed with this corrupted data. **CVE ID : CVE-2020-6096**		
gnutls					
gnutls					
Use of a Broken or Risky Cryptographic	03-04-2020	6.4	GnuTLS 3.6.x before 3.6.13 uses incorrect cryptography for DTLS. The earliest affected	N/A	A-GNU-GNUT-270420/513

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Algorithm			version is 3.6.3 (2018-07-16) because of an error in a 2017-10-06 commit. The DTLS client always uses 32 '\0' bytes instead of a random value, and thus contributes no randomness to a DTLS negotiation. This breaks the security guarantees of the DTLS protocol. **CVE ID : CVE-2020-11501**		
Google					
chrome					
Use After Free	13-04-2020	6.8	Use after free in audio in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6423**	N/A	A-GOO-CHRO-270420/514
Access of Resource Using Incompatible Type ('Type Confusion')	13-04-2020	6.8	Type Confusion in V8 in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6430**	N/A	A-GOO-CHRO-270420/515
Incorrect Default Permissions	13-04-2020	4.3	Insufficient policy enforcement in full screen in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to spoof security UI via a crafted HTML page.	N/A	A-GOO-CHRO-270420/516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-6431		
N/A	13-04-2020	4.3	Insufficient policy enforcement in navigations in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. **CVE ID : CVE-2020-6432**	N/A	A-GOO-CHRO-270420/517
N/A	13-04-2020	4.3	Insufficient policy enforcement in extensions in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. **CVE ID : CVE-2020-6433**	N/A	A-GOO-CHRO-270420/518
Use After Free	13-04-2020	6.8	Use after free in devtools in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6434**	N/A	A-GOO-CHRO-270420/519
N/A	13-04-2020	4.3	Insufficient policy enforcement in extensions in Google Chrome prior to 81.0.4044.92 allowed a remote attacker who had compromised the renderer process to bypass navigation restrictions via a crafted HTML page.	N/A	A-GOO-CHRO-270420/520

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-6435		
Use After Free	13-04-2020	6.8	Use after free in window management in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6436**	N/A	A-GOO-CHRO-270420/521
N/A	13-04-2020	4.3	Inappropriate implementation in WebView in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to spoof security UI via a crafted application. **CVE ID : CVE-2020-6437**	N/A	A-GOO-CHRO-270420/522
Information Exposure	13-04-2020	4.3	Insufficient policy enforcement in extensions in Google Chrome prior to 81.0.4044.92 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information from process memory via a crafted Chrome Extension. **CVE ID : CVE-2020-6438**	N/A	A-GOO-CHRO-270420/523
Incorrect Default Permissions	13-04-2020	6.8	Insufficient policy enforcement in navigations in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to bypass security UI via a crafted	N/A	A-GOO-CHRO-270420/524

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HTML page. **CVE ID : CVE-2020-6439**		
N/A	13-04-2020	4.3	Inappropriate implementation in extensions in Google Chrome prior to 81.0.4044.92 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information via a crafted Chrome Extension. **CVE ID : CVE-2020-6440**	N/A	A-GOO-CHRO-270420/525
Incorrect Default Permissions	13-04-2020	4.3	Insufficient policy enforcement in omnibox in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to bypass security UI via a crafted HTML page. **CVE ID : CVE-2020-6441**	N/A	A-GOO-CHRO-270420/526
Exposure of Resource to Wrong Sphere	13-04-2020	4.3	Inappropriate implementation in cache in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to leak cross-origin data via a crafted HTML page. **CVE ID : CVE-2020-6442**	N/A	A-GOO-CHRO-270420/527
Insufficient Verification of Data Authenticity	13-04-2020	6.8	Insufficient data validation in developer tools in Google Chrome prior to 81.0.4044.92 allowed a remote attacker who had convinced the user to use devtools to execute arbitrary code via	N/A	A-GOO-CHRO-270420/528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a crafted HTML page. **CVE ID : CVE-2020-6443**		
Out-of-bounds Write	13-04-2020	6.8	Uninitialized use in WebRTC in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6444**	N/A	A-GOO-CHRO-270420/529
Incorrect Default Permissions	13-04-2020	4.3	Insufficient policy enforcement in trusted types in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to bypass content security policy via a crafted HTML page. **CVE ID : CVE-2020-6445**	N/A	A-GOO-CHRO-270420/530
Incorrect Default Permissions	13-04-2020	4.3	Insufficient policy enforcement in trusted types in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to bypass content security policy via a crafted HTML page. **CVE ID : CVE-2020-6446**	N/A	A-GOO-CHRO-270420/531
Improper Restriction of Operations within the Bounds of a Memory Buffer	13-04-2020	6.8	Inappropriate implementation in developer tools in Google Chrome prior to 81.0.4044.92 allowed a remote attacker who had convinced the user to use devtools to potentially exploit heap corruption	N/A	A-GOO-CHRO-270420/532

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via a crafted HTML page. **CVE ID : CVE-2020-6447**		
Use After Free	13-04-2020	6.8	Use after free in V8 in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6448**	N/A	A-GOO-CHRO-270420/533
Use After Free	13-04-2020	6.8	Use after free in WebAudio in Google Chrome prior to 80.0.3987.162 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6450**	N/A	A-GOO-CHRO-270420/534
Use After Free	13-04-2020	6.8	Use after free in WebAudio in Google Chrome prior to 80.0.3987.162 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6451**	N/A	A-GOO-CHRO-270420/535
Out-of-bounds Write	13-04-2020	6.8	Heap buffer overflow in media in Google Chrome prior to 80.0.3987.162 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6452**	N/A	A-GOO-CHRO-270420/536
Use After Free	13-04-2020	6.8	Use after free in extensions in Google	N/A	A-GOO-CHRO-270420/537

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Chrome prior to 81.0.4044.92 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension. **CVE ID : CVE-2020-6454**		
Out-of-bounds Read	13-04-2020	6.8	Out of bounds read in WebSQL in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6455**	N/A	A-GOO-CHRO-270420/538
Incorrect Default Permissions	13-04-2020	4.3	Insufficient validation of untrusted input in clipboard in Google Chrome prior to 81.0.4044.92 allowed a local attacker to bypass site isolation via crafted clipboard contents. **CVE ID : CVE-2020-6456**	N/A	A-GOO-CHRO-270420/539
gpac					
gpac					
Use After Free	05-04-2020	7.5	An issue was discovered in libgpac.a in GPAC 0.8.0, as demonstrated by MP4Box. audio_sample_entry_Read in isomedia/box_code_base.c does not properly decide when to make gf_isom_box_del calls. This	N/A	A-GPA-GPAC-270420/540

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leads to various use-after-free outcomes involving mdia_Read, gf_isom_delete_movie, and gf_isom_parse_movie_boxes. **CVE ID : CVE-2020-11558**		
greenbrowser_project					
greenbrowser					
Missing Authorization	08-04-2020	4.3	GreenBrowser before version 1.2 has a vulnerability where apps that rely on URL Parsing to verify that a given URL is pointing to a trust server may be susceptible to many different ways to get URL parsing and verification wrong, which allows an attacker to circumvent the access control. This problem has been patched in version 1.2. **CVE ID : CVE-2020-11000**	https://github.com/luchua-bc/GreenBrowser/security/advisories/GHSA-7x3j-7x5w-8g7w	A-GRE-GREE-270420/541
Haproxy					
haproxy					
Out-of-bounds Write	02-04-2020	6.5	In hpack_dht_insert in hpack-tbl.c in the HPACK decoder in HAProxy 1.8 through 2.x before 2.1.4, a remote attacker can write arbitrary bytes around a certain location on the heap via a crafted HTTP/2 request, possibly causing	https://bugzilla.redhat.com/show_bug.cgi?id=1819111, https://bugzilla.suse.com/show_bug.cgi?id=11	A-HAP-HAPR-270420/542

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote code execution. **CVE ID : CVE-2020-11100**	68023, https://git.haproxy.org/?p=haproxy.git;a=commit;h=5dfc5d5cd0d2128d77253ead3acf03a421ab5b88, https://www.haproxy.org/download/2.1/src/CHANGELOG	
heroku-addonpool_project					
heroku-addonpool					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-04-2020	7.5	heroku-addonpool through 0.1.15 is vulnerable to Command Injection. **CVE ID : CVE-2020-7634**	N/A	A-HER-HERO-270420/543
Honeywell					
notifier_webserver					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-04-2020	7.5	Honeywell Notifier Web Server (NWS) Version 3.50 is vulnerable to a path traversal attack, which allows an attacker to bypass access to restricted directories. Honeywell has released a firmware update to address the problem. **CVE ID : CVE-2020-6974**	N/A	A-HON-NOTI-270420/544

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
IBM					
strongloop_nginx_controller					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	02-04-2020	7.5	strong-nginx-controller through 1.0.2 is vulnerable to Command Injection. It allows execution of arbitrary command as part of the '_nginxCmd()' function. **CVE ID : CVE-2020-7621**	N/A	A-IBM-STRO-270420/545
spectrum_scale					
Improper Privilege Management	03-04-2020	6.9	IBM Spectrum Scale 4.2 and 5.0 could allow a local unprivileged attacker with intimate knowledge of the enviornment to execute commands as root using specially crafted input. IBM X-Force ID: 175977. **CVE ID : CVE-2020-4273**	https://www.ibm.com/support/pages/node/6151701	A-IBM-SPEC-270420/546
websphere_application_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-04-2020	4.3	IBM WebSphere Application Server - Liberty 17.0.0.3 through 20.0.0.3 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: 176668. **CVE ID : CVE-2020-4303**	https://www.ibm.com/support/pages/node/6147195	A-IBM-WEBS-270420/547
Improper	02-04-2020	4.3	IBM WebSphere	https://ww	A-IBM-WEBS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			Application Server - Liberty 17.0.0.3 through 20.0.0.3 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: 176670. **CVE ID : CVE-2020-4304**	w.ibm.com/support/pages/node/6147195	270420/548
Improper Privilege Management	10-04-2020	6.5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 traditional is vulnerable to a privilege escalation vulnerability when using token-based authentication in an admin request over the SOAP connector. IBM X-Force ID: 178929. **CVE ID : CVE-2020-4362**	https://www.ibm.com/support/pages/node/6174417	A-IBM-WEBS-270420/549
security_information_queue					
Information Exposure	08-04-2020	4	IBM Security Information Queue (ISIQ) 1.0.0, 1.0.1, 1.0.2, 1.0.3, 1.0.4, and 1.0.5 could expose sensitive information from applicatino errors which could be used in further attacks against the system. IBM X-Force ID: 174400. **CVE ID : CVE-2020-4164**	https://www.ibm.com/support/pages/node/6172605	A-IBM-SECU-270420/550
Improper	08-04-2020	4	IBM Security Information	https://ww	A-IBM-SECU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication			Queue (ISIQ) 1.0.0, 1.0.1, 1.0.2, 1.0.3, 1.0.4, and 1.0.5 could allow an authenticated user to perform unauthorized actions by bypassing illegal character restrictions. X-Force ID: 176205. **CVE ID : CVE-2020-4282**	w.ibm.com/support/pages/node/6172587	270420/551
Information Exposure	08-04-2020	5	IBM Security Information Queue (ISIQ) 1.0.0, 1.0.1, 1.0.2, 1.0.3, 1.0.4, and 1.0.5 could disclose sensitive information to an unauthorized user due to insufficient timeout functionality in the Web UI. IBM X-Force ID: 176207. **CVE ID : CVE-2020-4284**	https://www.ibm.com/support/pages/node/6172551	A-IBM-SECU-270420/552
Information Exposure	08-04-2020	5	IBM Security Information Queue (ISIQ) 1.0.0, 1.0.1, 1.0.2, 1.0.3, 1.0.4, and 1.0.5 could allow a remote attacker to obtain sensitive information, caused by the failure to set the HTTPOnly flag. A remote attacker could exploit this vulnerability to obtain sensitive information from the cookie. IBM X-Force ID: 176332. **CVE ID : CVE-2020-4289**	https://www.ibm.com/support/pages/node/6172593	A-IBM-SECU-270420/553
Authentication Bypass by Spoofing	08-04-2020	5.5	IBM Security Information Queue (ISIQ) 1.0.0, 1.0.1, 1.0.2, 1.0.3, 1.0.4, and	https://www.ibm.com/support/pa	A-IBM-SECU-270420/554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.5 could allow any authenticated user to spoof the configuration owner of any other user which disclose sensitive information or allow for unauthorized access. IBM X-Force ID: 176333. **CVE ID : CVE-2020-4290**	ges/node/6172599	
Session Fixation	08-04-2020	4.3	IBM Security Information Queue (ISIQ) 1.0.0, 1.0.1, 1.0.2, 1.0.3, 1.0.4, and 1.0.5 could disclose sensitive information to an unauthorized user due to insufficient timeout functionality in the Web UI. IBM X-Force ID: 176334. **CVE ID : CVE-2020-4291**	https://www.ibm.com/support/pages/node/6172545	A-IBM-SECU-270420/555
rational_doors_next_generation					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-04-2020	3.5	IBM DOORS Next Generation (DNG/RRC) 6.0.2. 6.0.6, and 6.0.61 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: 175490. **CVE ID : CVE-2020-4252**	https://www.ibm.com/support/pages/node/6172635	A-IBM-RATI-270420/556
qradar_security_information_and_event_manager					
Missing	14-04-2020	4	IBM QRadar SIEM 7.3.0 through 7.3.3 could allow	https://www.ibm.com/	A-IBM-QRAD-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authorization			an authenticated attacker to perform unauthorized actions due to improper input validation. IBM X-Force ID: 174201. **CVE ID : CVE-2020-4151**	support/pages/node/6189675	270420/557
doors_next_generation					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-04-2020	3.5	IBM DOORS Next Generation (DNG/RRC) 6.0.2. 6.0.6, and 6.0.61 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: 175490. **CVE ID : CVE-2020-4252**	https://www.ibm.com/support/pages/node/6172635	A-IBM-DOOR-270420/558
cloud_pak_for_automation					
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-04-2020	4	The IBM Process Federation Server 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, and 19.0.0.3 Global Teams REST API does not properly shutdown the thread pools that it creates to retrieve Global Teams information from the federated systems. As a consequence, the Java Virtual Machine can't recover the memory used by those thread pools, which leads to an	https://www.ibm.com/support/pages/node/6125403	A-IBM-CLOU-270420/559

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			OutOfMemory exception when the Process Federation Server Global Teams REST API is used extensively. IBM X-Force ID: 177596. **CVE ID : CVE-2020-4325**		
process_federation_server					
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-04-2020	4	The IBM Process Federation Server 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, and 19.0.0.3 Global Teams REST API does not properly shutdown the thread pools that it creates to retrieve Global Teams information from the federated systems. As a consequence, the Java Virtual Machine can't recover the memory used by those thread pools, which leads to an OutOfMemory exception when the Process Federation Server Global Teams REST API is used extensively. IBM X-Force ID: 177596. **CVE ID : CVE-2020-4325**	https://www.ibm.com/support/pages/node/6125403	A-IBM-PROC-270420/560
idxbroker					
impress_for_idx_broker					
Improper Authentication	07-04-2020	4	An issue was discovered in the IMPress for IDX Broker plugin before 2.6.2 for WordPress. wrappers.php allows a logged-in user (with the	N/A	A-IDX-IMPR-270420/561

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Subscriber role) to permanently delete arbitrary posts and pages, create new posts with arbitrary subjects, and modify the subjects of existing posts and pages (via create_dynamic_page and delete_dynamic_page). **CVE ID : CVE-2020-9514**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-04-2020	3.5	Stored XSS in the IMPress for IDX Broker WordPress plugin before 2.6.2 allows authenticated attackers with minimal (subscriber-level) permissions to save arbitrary JavaScript in the plugin's settings panel via the idx_update_recaptcha_key AJAX action and a crafted idx_recaptcha_site_key parameter, which would then be executed in the browser of any administrator visiting the panel. This could be used to create new administrator-level accounts. **CVE ID : CVE-2020-11512**	N/A	A-IDX-IMPR-270420/562
ini-parser_project					
ini-parser					
Improperly Controlled Modification of Dynamically-	02-04-2020	7.5	ini-parser through 0.0.2 is vulnerable to Prototype Pollution.The library could be tricked into	https://github.com/rawiroaisen/node-ini-	A-INI-INI--270420/563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Determined Object Attributes			adding or modifying properties of Object.prototype using a '__proto__' payload. **CVE ID : CVE-2020-7617**	parser/blob/master/index.js#L14, https://snyk.io/vuln/SNYK-JS-INIPARSER-564122	
install-package_project					
install-package					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	02-04-2020	7.5	install-package through 1.1.6 is vulnerable to Command Injection. It allows execution of arbitrary commands via the device function. **CVE ID : CVE-2020-7628**	N/A	A-INS-INST-270420/564
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	02-04-2020	7.5	install-package through 0.4.0 is vulnerable to Command Injection. It allows execution of arbitrary commands via the options argument. **CVE ID : CVE-2020-7629**	N/A	A-INS-INST-270420/565
ivanti					
workspace_control					
Information Exposure	04-04-2020	2.1	Ivanti Workspace Control before 10.4.30.0, when SCCM integration is enabled, allows local users to obtain sensitive information (keying material). **CVE ID : CVE-2020-11533**	N/A	A-IVA-WORK-270420/566
Jenkins					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
code_coverage_api					
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	07-04-2020	4	Jenkins Code Coverage API Plugin 1.1.4 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks. **CVE ID : CVE-2020-2172**	https://jenkins.io/security/advisory/2020-04-07/#SECURITY-1699	A-JEN-CODE-270420/567
fitnesse					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-04-2020	3.5	Jenkins FitNesse Plugin 1.31 and earlier does not correctly escape report contents before showing them on the Jenkins UI, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by users able to control the XML input files processed by the plugin. **CVE ID : CVE-2020-2175**	https://jenkins.io/security/advisory/2020-04-07/#SECURITY-1801	A-JEN-FITN-270420/568
gatling					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-04-2020	3.5	Jenkins Gatling Plugin 1.2.7 and earlier prevents Content-Security-Policy headers from being set for Gatling reports served by the plugin, resulting in an XSS vulnerability exploitable by users able to change report content. **CVE ID : CVE-2020-2173**	https://jenkins.io/security/advisory/2020-04-07/#SECURITY-1633	A-JEN-GATL-270420/569
awseb_deployment					
Improper Neutralization of Input During Web Page	07-04-2020	4.3	Jenkins AWSEB Deployment Plugin 0.3.19 and earlier does not escape various values	https://jenkins.io/security/advisory/2020-04-	A-JEN-AWSE-270420/570

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			printed as part of form validation output, resulting in a reflected cross-site scripting vulnerability. **CVE ID : CVE-2020-2174**	07/#SECURITY-1769	
usemango_runner					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-04-2020	3.5	Multiple form validation endpoints in Jenkins useMango Runner Plugin 1.4 and earlier do not escape values received from the useMango service, resulting in a cross-site scripting (XSS) vulnerability exploitable by users able to control the values returned from the useMango service. **CVE ID : CVE-2020-2176**	https://jenkins.io/security/advisory/2020-04-07/#SECURITY-1780	A-JEN-USEM-270420/571
Jetbrains					
pycharm					
Insufficiently Protected Credentials	10-04-2020	5	In JetBrains PyCharm 2019.2.5 and 2019.3 on Windows, Apple Notarization Service credentials were included. This is fixed in 2019.2.6 and 2019.3.3. **CVE ID : CVE-2020-11694**	N/A	A-JET-PYCH-270420/572
jooby					
jooby					
Inconsistent Interpretation of HTTP Requests ('HTTP	06-04-2020	7.5	All versions of Jooby before 2.2.1 are vulnerable to HTTP Response Splitting. The DefaultHttpHeaders is set	N/A	A-JOO-JOOB-270420/573

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Request Smuggling')			to false which means it does not validates that the header isn't being abused for HTTP Response Splitting. **CVE ID : CVE-2020-7622**		
jscover_project					
jscover					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	02-04-2020	7.5	jscover through 1.0.0 is vulnerable to Command Injection. It allows execution of arbitrary command via the source argument. **CVE ID : CVE-2020-7623**	N/A	A-JSC-JSCO-270420/574
Juniper					
junos					
Improper Authentication	08-04-2020	6.9	On Juniper Networks EX and QFX Series, an authentication bypass vulnerability may allow a user connected to the console port to login as root without any password. This issue might only occur in certain scenarios: • At the first reboot after performing device factory reset using the command “request system zeroize”; or • A temporary moment during the first reboot after the software upgrade when the device configured in Virtual Chassis mode. This issue affects Juniper Networks	https://kb.juniper.net/JSA11001	A-JUN-JUNO-270420/575

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Junos OS on EX and QFX Series: 14.1X53 versions prior to 14.1X53-D53; 15.1 versions prior to 15.1R7-S4; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S4; 17.1 versions prior to 17.1R2-S11, 17.1R3-S1; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S6; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S8; 18.2 versions prior to 18.2R2; 18.3 versions prior to 18.3R1-S7, 18.3R2. This issue does not affect Juniper Networks Junos OS 12.3. **CVE ID : CVE-2020-1618**		
Improper Privilege Management	08-04-2020	4.6	A privilege escalation vulnerability in Juniper Networks QFX10K Series, EX9200 Series, MX Series, and PTX Series with Next-Generation Routing Engine (NG-RE), allows a local authenticated high privileged user to access the underlying WRL host. This issue only affects QFX10K Series with NG-RE, EX9200 Series with NG-RE, MX Series with NG-RE and PTX Series with NG-RE; which uses vmhost. This issue affects Juniper Networks Junos	https://kb.juniper.net/JSA11002	A-JUN-JUNO-270420/576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			OS: 16.1 versions prior to 16.1R7-S6; 16.2 versions prior to 16.2R2-S11; 17.1 versions prior to 17.1R2-S11, 17.1R3; 17.2 versions prior to 17.2R1-S9, 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S7, 17.4R3; 18.1 versions prior to 18.1R3-S4; 18.2 versions prior to 18.2R3; 18.2X75 versions prior to 18.2X75-D50; 18.3 versions prior to 18.3R2; 18.4 versions prior to 18.4R2. To identify whether the device has NG-RE with vmhost, customer can run the following command: > show vmhost status Compute cluster: rainier-re-cc Compute Node: rainier-re-cn, Online If the "show vmhost status" is not supported, then the device does not have NG-RE with vmhost. **CVE ID : CVE-2020-1619**		
Uncontrolled Resource Consumption	08-04-2020	3.3	The kernel memory usage represented as "temp" via 'show system virtual-memory' may constantly increase when Integrated Routing and Bridging (IRB) is configured with multiple underlay physical interfaces, and one interface flaps. This	https://kb.juniper.net/JSA11004	A-JUN-JUNO-270420/577

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory leak can affect running daemons (processes), leading to an extended Denial of Service (DoS) condition. Usage of "temp" virtual memory, shown here by a constantly increasing value of outstanding Requests, can be monitored by executing the 'show system virtual-memory' command as shown below: user@junos> show system virtual-memory |match "fpc|type|temp" fpc0: ---------- ---------- Type InUse MemUse HighUse Requests Size(s) temp 2023 431K - 10551 16,32,64,128,256,512,1024,2048,4096,65536,262144,1048576,2097152,4194304,8388608 fpc1: ---------- ---------- - Type InUse MemUse HighUse Requests Size(s) temp 2020 431K - 6460 16,32,64,128,256,512,1024,2048,4096,65536,262144,1048576,2097152,4194304,8388608 user@junos> show system virtual-memory |match "fpc|type|temp" fpc0: ---------- ----------		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			---------- Type InUse MemUse HighUse Requests Size(s) temp 2023 431K - 16101 16,32,64,128,256,512,1024,2048,4096,65536,262144,1048576,2097152,4194304,8388608 fpc1: ---------- - Type InUse MemUse HighUse Requests Size(s) temp 2020 431K - 6665 16,32,64,128,256,512,1024,2048,4096,65536,262144,1048576,2097152,4194304,8388608 user@junos> show system virtual-memory |match "fpc|type|temp" fpc0: ---------- ---------- Type InUse MemUse HighUse Requests Size(s) temp 2023 431K - 21867 16,32,64,128,256,512,1024,2048,4096,65536,262144,1048576,2097152,4194304,8388608 fpc1: ---------- - Type InUse MemUse HighUse Requests Size(s) temp 2020 431K - 6858 16,32,64,128,256,512,1024,2048,4096,65536,262144,1048576,2097152,4194304,8388608 This issue affects Juniper Networks Junos OS: 16.1 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 16.1R7-S6; 17.1 versions prior to 17.1R2-S11, 17.1R3-S1; 17.2 versions prior to 17.2R2-S8, 17.2R3-S3; 17.2X75 versions prior to 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S6; 17.4 versions prior to 17.4R2-S5, 17.4R3; 18.1 versions prior to 18.1R3-S7; 18.2 versions prior to 18.2R2-S5, 18.2R3; 18.2X75 versions prior to 18.2X75-D33, 18.2X75-D411, 18.2X75-D420, 18.2X75-D60; 18.3 versions prior to 18.3R1-S5, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R2-S2, 18.4R3; 19.1 versions prior to 19.1R1-S3, 19.1R2; 19.2 versions prior to 19.2R1-S3, 19.2R2. This issue does not affect Juniper Networks Junos OS 12.3 and 15.1. **CVE ID : CVE-2020-1625**		
Improper Input Validation	08-04-2020	5	A vulnerability in Juniper Networks Junos OS on vMX and MX150 devices may allow an attacker to cause a Denial of Service (DoS) by sending specific packets requiring special processing in microcode that the flow cache can't handle, causing the riot forwarding daemon to crash. By continuously	https://kb.juniper.net/JSA11006	A-JUN-JUNO-270420/578

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sending the same specific packets, an attacker can repeatedly crash the riot process causing a sustained Denial of Service. Flow cache is specific to vMX based products and the MX150, and is enabled by default in performance mode. This issue can only be triggered by traffic destined to the device. Transit traffic will not cause the riot daemon to crash. When the issue occurs, a core dump and riot log file entry are generated. For example: /var/crash/core.J-UKERN.mpc0.1557255993.3864.gz /home/pfe/RIOT logs: fpc0 riot[1888]: PANIC in lu_reorder_send_packet_postproc(): fpc0 riot[6655]: PANIC in lu_reorder_send_packet_postproc(): This issue affects Juniper Networks Junos OS: 18.1 versions prior to 18.1R3 on vMX and MX150; 18.2 versions prior to 18.2R3 on vMX and MX150; 18.2X75 versions prior to 18.2X75-D60 on vMX and MX150; 18.3 versions prior to 18.3R3 on vMX and MX150; 18.4 versions prior to 18.4R2 on vMX		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and MX150; 19.1 versions prior to 19.1R2 on vMX and MX150. This issue does not affect Junos OS versions prior to 18.1R1. **CVE ID : CVE-2020-1627**		
Information Exposure	08-04-2020	5	Juniper Networks Junos OS uses the 128.0.0.0/2 subnet for internal communications between the RE and PFEs. It was discovered that packets utilizing these IP addresses may egress an EX4300 switch, leaking configuration information such as heartbeats, kernel versions, etc. out to the Internet, leading to an information exposure vulnerability. This issue affects Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D53 on EX4300; 15.1 versions prior to 15.1R7-S6 on EX4300; 15.1X49 versions prior to 15.1X49-D200, 15.1X49-D210 on EX4300; 16.1 versions prior to 16.1R7-S7 on EX4300; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2 on EX4300; 17.2 versions prior to 17.2R3-S3 on EX4300; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7 on EX4300; 17.4 versions prior to 17.4R2-S9, 17.4R3 on EX4300; 18.1	https://kb.juniper.net/JSA11008	A-JUN-JUNO-270420/579

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 18.1R3-S8 on EX4300; 18.2 versions prior to 18.2R3-S2 on EX4300; 18.3 versions prior to 18.3R2-S3, 18.3R3, 18.3R3-S1 on EX4300; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R3 on EX4300; 19.1 versions prior to 19.1R1-S4, 19.1R2 on EX4300; 19.2 versions prior to 19.2R1-S4, 19.2R2 on EX4300; 19.3 versions prior to 19.3R1-S1, 19.3R2 on EX4300. **CVE ID : CVE-2020-1628**		
Time-of-check Time-of-use (TOCTOU) Race Condition	08-04-2020	4.3	A race condition vulnerability on Juniper Network Junos OS devices may cause the routing protocol daemon (RPD) process to crash and restart while processing a BGP NOTIFICATION message. This issue affects Juniper Networks Junos OS: 16.1 versions prior to 16.1R7-S6; 16.2 versions prior to 16.2R2-S11; 17.1 versions prior to 17.1R2-S11, 17.1R3-S1; 17.2 versions prior to 17.2R1-S9, 17.2R3-S3; 17.2 version 17.2R2 and later versions; 17.2X75 versions prior to 17.2X75-D105, 17.2X75-D110; 17.3 versions prior to 17.3R2-S5, 17.3R3-S6;	https://kb.juniper.net/JSA11009	A-JUN-JUNO-270420/580

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			17.4 versions prior to 17.4R2-S7, 17.4R3; 18.1 versions prior to 18.1R3-S8; 18.2 versions prior to 18.2R3-S3; 18.2X75 versions prior to 18.2X75-D410, 18.2X75-D420, 18.2X75-D50, 18.2X75-D60; 18.3 versions prior to 18.3R1-S5, 18.3R2-S2, 18.3R3; 18.4 versions prior to 18.4R2-S2, 18.4R3; 19.1 versions prior to 19.1R1-S2, 19.1R2; 19.2 versions prior to 19.2R1-S4, 19.2R2. This issue does not affect Juniper Networks Junos OS prior to version 16.1R1. **CVE ID : CVE-2020-1629**		
Improper Privilege Management	08-04-2020	2.1	A privilege escalation vulnerability in Juniper Networks Junos OS devices configured with dual Routing Engines (RE), Virtual Chassis (VC) or high-availability cluster may allow a local authenticated low-privileged user with access to the shell to perform unauthorized configuration modification. This issue does not affect Junos OS device with single RE or stand-alone configuration. This issue affects Juniper Networks Junos OS 12.3 versions prior to	https://kb.juniper.net/JSA11010	A-JUN-JUNO-270420/581

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12.3R12-S14; 12.3X48 versions prior to 12.3X48-D86, 12.3X48-D90; 14.1X53 versions prior to 14.1X53-D51; 15.1 versions prior to 15.1R7-S6; 15.1X49 versions prior to 15.1X49-D181, 15.1X49-D190; 15.1X53 versions prior to 15.1X53-D592; 16.1 versions prior to 16.1R4-S13, 16.1R7-S6; 16.2 versions prior to 16.2R2-S10; 17.1 versions prior to 17.1R2-S11, 17.1R3-S1; 17.2 versions prior to 17.2R1-S9, 17.2R3-S3; 17.3 versions prior to 17.3R3-S6; 17.4 versions prior to 17.4R2-S6, 17.4R3; 18.1 versions prior to 18.1R3-S7; 18.2 versions prior to 18.2R2-S5, 18.2R3-S1; 18.2 versions prior to 18.2X75-D12, 18.2X75-D33, 18.2X75-D420, 18.2X75-D60, 18.2X75-D411; 18.3 versions prior to 18.3R1-S5, 18.3R2-S1, 18.3R3; 18.4 versions prior to 18.4R1-S4, 18.4R2-S1, 18.4R3; 19.1 versions prior to 19.1R1-S2, 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. **CVE ID : CVE-2020-1630**		
Improper Input	09-04-2020	3.3	Due to a new NDP proxy feature for EVPN leaf nodes introduced in Junos	https://kb.juniper.net/J	A-JUN-JUNO-270420/582

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			OS 17.4, crafted NDPv6 packets could transit a Junos device configured as a Broadband Network Gateway (BNG) and reach the EVPN leaf node, causing a stale MAC address entry. This could cause legitimate traffic to be discarded, leading to a Denial of Service (DoS) condition. This issue only affects Junos OS 17.4 and later releases. Prior releases do not support this feature and are unaffected by this vulnerability. This issue only affects IPv6. IPv4 ARP proxy is unaffected by this vulnerability. This issue affects Juniper Networks Junos OS: 17.4 versions prior to 17.4R2-S9, 17.4R3 on MX Series; 18.1 versions prior to 18.1R3-S9 on MX Series; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D33, 18.2X75-D411, 18.2X75-D420, 18.2X75-D60 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3 on MX Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S2, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2 on	SA11012	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series. **CVE ID : CVE-2020-1633**		
Improper Authentication	08-04-2020	5.8	A vulnerability in Juniper Networks SRX Series device configured as a Junos OS Enforcer device may allow a user to access network resources that are not permitted by a UAC policy. This issue might occur when the IP address range configured in the Infranet Controller (IC) is configured as an IP address range instead of an IP address/netmask. See the Workaround section for more detail. The Junos OS Enforcer CLI settings are disabled by default. This issue affects Juniper Networks Junos OS on SRX Series: 12.3X48 versions prior to 12.3X48-D100; 15.1X49 versions prior to 15.1X49-D210; 17.3 versions prior to 17.3R2-S5, 17.3R3-S8; 17.4 versions prior to 17.4R2-S9, 17.4R3-S1; 18.1 versions prior to 18.1R3-S10; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R3-S2; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3-S1; 19.1 versions prior to	https://kb.juniper.net/JSA11018	A-JUN-JUNO-270420/583

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.1R1-S4, 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S3, 19.2R2; 19.3 versions prior to 19.3R2-S1, 19.3R3; 19.4 versions prior to 19.4R1-S1, 19.4R2. **CVE ID : CVE-2020-1637**		
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1	https://kb.juniper.net/JSA10996	A-JUN-JUNO-270420/584

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
Use of Hard-coded Credentials	08-04-2020	10	The factory configuration for vMX installations, as shipped, includes default credentials for the root account. Without proper modification of these default credentials by the administrator, an attacker could exploit these credentials and access the vMX instance without authorization. This issue	https://kb.juniper.net/JSA10998	A-JUN-JUNO-270420/585

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affects Juniper Networks Junos OS: 17.1 versions prior to 17.1R2-S11, 17.1R3-S2 on vMX; 17.2 versions prior to 17.2R3-S3 on vMX; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7 on vMX; 17.4 versions prior to 17.4R2-S9, 17.4R3 on vMX; 18.1 versions prior to 18.1R3-S9 on vMX; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3 on vMX; 18.2X75 versions prior to 18.2X75-D420, 18.2X75-D60 on vMX; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1 on vMX; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R3 on vMX; 19.1 versions prior to 19.1R1-S4, 19.1R2, 19.1R3 on vMX; 19.2 versions prior to 19.2R1-S3, 19.2R2 on vMX; 19.3 versions prior to 19.3R1-S1, 19.3R2 on vMX. **CVE ID : CVE-2020-1615**		
Improper Initialization	08-04-2020	7.8	This issue occurs on Juniper Networks Junos OS devices which do not support Advanced Forwarding Interface (AFI) / Advanced Forwarding Toolkit (AFT). Devices using AFI and AFT are not exploitable to this issue. An improper initialization	N/A	A-JUN-JUNO-270420/586

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of memory in the packet forwarding architecture in Juniper Networks Junos OS non-AFI/AFT platforms which may lead to a Denial of Service (DoS) vulnerability being exploited when a genuine packet is received and inspected by non-AFT/AFI sFlow and when the device is also configured with firewall policers. This first genuine packet received and inspected by sampled flow (sFlow) through a specific firewall policer will cause the device to reboot. After the reboot has completed, if the device receives and sFlow inspects another genuine packet seen through a specific firewall policer, the device will generate a core file and reboot. Continued inspection of these genuine packets will create an extended Denial of Service (DoS) condition. Depending on the method for service restoration, e.g. hard boot or soft reboot, a core file may or may not be generated the next time the packet is received and inspected by sFlow. This issue affects: Juniper Networks Junos OS 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 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.1 versions prior to 18.1R3-S9 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.2X75 versions prior to 18.2X75-D12, 18.2X75-D30 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.2 versions prior to 18.2R3 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.3 versions prior to 18.3R3 on PTX1000 and PTX10000 Series, QFX10000 Series. This issue is not applicable to Junos OS versions before 17.4R1. This issue is not applicable to Junos OS Evolved or Junos OS with Advanced Forwarding Toolkit (AFT) forwarding implementations which use a different implementation of sFlow. The following example information is unrelated to this issue and is provided solely to assist you with determining if you have AFT or not. Example: A Junos OS device which supports the use of EVPN signaled VPWS with Flexible Cross		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connect uses the AFT implementation. Since this configuration requires support and use of the AFT implementation to support this configuration, the device is not vulnerable to this issue as the sFlow implementation is different using the AFT architecture. For further details about AFT visit the AFI / AFT are in the links below. If you are uncertain if you use the AFI/AFT implementation or not, there are configuration examples in the links below which you may use to determine if you are vulnerable to this issue or not. If the commands work, you are. If not, you are not. You may also use the Feature Explorer to determine if AFI/AFT is supported or not. If you are still uncertain, please contact your support resources. **CVE ID : CVE-2020-1617**		
vmx					
Improper Input Validation	08-04-2020	5	A vulnerability in Juniper Networks Junos OS on vMX and MX150 devices may allow an attacker to cause a Denial of Service (DoS) by sending specific	https://kb.juniper.net/JSA11006	A-JUN-VMX-270420/587

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			packets requiring special processing in microcode that the flow cache can't handle, causing the riot forwarding daemon to crash. By continuously sending the same specific packets, an attacker can repeatedly crash the riot process causing a sustained Denial of Service. Flow cache is specific to vMX based products and the MX150, and is enabled by default in performance mode. This issue can only be triggered by traffic destined to the device. Transit traffic will not cause the riot daemon to crash. When the issue occurs, a core dump and riot log file entry are generated. For example: /var/crash/core.J-UKERN.mpc0.1557255993.3864.gz /home/pfe/RIOT logs: fpc0 riot[1888]: PANIC in lu_reorder_send_packet_postproc(): fpc0 riot[6655]: PANIC in lu_reorder_send_packet_postproc(): This issue affects Juniper Networks Junos OS: 18.1 versions prior to 18.1R3 on vMX and MX150; 18.2 versions prior to 18.2R3 on vMX and MX150; 18.2X75		

CVSS Scoring Scale	0-1	1-2	2-3	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 18.2X75-D60 on vMX and MX150; 18.3 versions prior to 18.3R3 on vMX and MX150; 18.4 versions prior to 18.4R2 on vMX and MX150; 19.1 versions prior to 19.1R2 on vMX and MX150. This issue does not affect Junos OS versions prior to 18.1R1. **CVE ID : CVE-2020-1627**		
Use of Hard-coded Credentials	08-04-2020	10	The factory configuration for vMX installations, as shipped, includes default credentials for the root account. Without proper modification of these default credentials by the administrator, an attacker could exploit these credentials and access the vMX instance without authorization. This issue affects Juniper Networks Junos OS: 17.1 versions prior to 17.1R2-S11, 17.1R3-S2 on vMX; 17.2 versions prior to 17.2R3-S3 on vMX; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7 on vMX; 17.4 versions prior to 17.4R2-S9, 17.4R3 on vMX; 18.1 versions prior to 18.1R3-S9 on vMX; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3 on vMX; 18.2X75 versions prior to 18.2X75-D420, 18.2X75-D60 on vMX; 18.3	https://kb.juniper.net/JSA10998	A-JUN-VMX-270420/588

CVSS Scoring Scale	0-1	1-2	2-3	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 18.3R1-S7, 18.3R2-S3, 18.3R3-S1 on vMX; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R3 on vMX; 19.1 versions prior to 19.1R1-S4, 19.1R2, 19.1R3 on vMX; 19.2 versions prior to 19.2R1-S3, 19.2R2 on vMX; 19.3 versions prior to 19.3R1-S1, 19.3R2 on vMX. **CVE ID : CVE-2020-1615**		
advanced_threat_protection					
Improper Restriction of Excessive Authentication Attempts	08-04-2020	5	Due to insufficient server-side login attempt limit enforcement, a vulnerability in the SSH login service of Juniper Networks Juniper Advanced Threat Prevention (JATP) Series and Virtual JATP (vJATP) devices allows an unauthenticated, remote attacker to perform multiple login attempts in excess of the configured login attempt limit. Successful exploitation will allow the attacker to perform brute-force password attacks on the SSH service. This issue affects: Juniper Networks JATP and vJATP versions prior to 5.0.6.0. **CVE ID : CVE-2020-1616**	N/A	A-JUN-ADVA-270420/589
virtual_advanced_threat_protection					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Excessive Authentication Attempts	08-04-2020	5	Due to insufficient server-side login attempt limit enforcement, a vulnerability in the SSH login service of Juniper Networks Juniper Advanced Threat Prevention (JATP) Series and Virtual JATP (vJATP) devices allows an unauthenticated, remote attacker to perform multiple login attempts in excess of the configured login attempt limit. Successful exploitation will allow the attacker to perform brute-force password attacks on the SSH service. This issue affects: Juniper Networks JATP and vJATP versions prior to 5.0.6.0. **CVE ID : CVE-2020-1616**	N/A	A-JUN-VIRT-270420/590
karma-mojo_project					
karma-mojo					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	02-04-2020	7.5	karma-mojo through 1.0.1 is vulnerable to Command Injection. It allows execution of arbitrary commands via the config argument. **CVE ID : CVE-2020-7626**	N/A	A-KAR-KARM-270420/591
konghq					
docker-kong					
N/A	12-04-2020	7.5	An issue was discovered in docker-kong (for Kong) through 2.0.3. The admin	N/A	A-KON-DOCK-270420/592

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			API port may be accessible on interfaces other than 127.0.0.1. **CVE ID : CVE-2020-11710**		
learndash					
learndash					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-04-2020	7.5	LearnDash Wordpress plugin version below 3.1.6 is vulnerable to Unauthenticated SQL Injection. **CVE ID : CVE-2020-6009**	N/A	A-LEA-LEAR-270420/593
libsixel_project					
libsixel					
Access of Uninitialized Pointer	12-04-2020	4.3	load_png in loader.c in libsixel.a in libsixel 1.8.6 has an uninitialized pointer leading to an invalid call to free, which can cause a denial of service. **CVE ID : CVE-2020-11721**	N/A	A-LIB-LIBS-270420/594
Libssh					
libssh					
Uncontrolled Resource Consumption	13-04-2020	5	A flaw was found in libssh versions before 0.8.9 and before 0.9.4 in the way it handled AES-CTR (or DES ciphers if enabled) ciphers. The server or client could crash when the connection hasn't been fully initialized and the system tries to	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1730	A-LIB-LIBS-270420/595

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cleanup the ciphers when closing the connection. The biggest threat from this vulnerability is system availability. **CVE ID : CVE-2020-1730**		
Limesurvey					
limesurvey					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-04-2020	5	LimeSurvey before 4.1.12+200324 contains a path traversal vulnerability in application/controllers/admin/LimeSurveyFileManager.php. **CVE ID : CVE-2020-11455**	N/A	A-LIM-LIME-270420/596
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-04-2020	4.3	LimeSurvey before 4.1.12+200324 has stored XSS in application/views/admin/surveysgroups/surveySettings.php and application/models/SurveysGroups.php (aka survey groups). **CVE ID : CVE-2020-11456**	N/A	A-LIM-LIME-270420/597
Linuxfoundation					
argo_continuous_delivery					
Session Fixation	08-04-2020	5	As of v1.5.0, the Argo web interface authentication system issued immutable tokens. Authentication tokens, once issued, were usable forever without expiration—there was no refresh or forced re-	N/A	A-LIN-ARGO-270420/598

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authentication. **CVE ID : CVE-2020-8826**		
Improper Authentication	08-04-2020	5	As of v1.5.0, the Argo API does not implement anti-automation measures such as rate limiting, account lockouts, or other anti-bruteforce measures. Attackers can submit an unlimited number of authentication attempts without consequence. **CVE ID : CVE-2020-8827**	N/A	A-LIN-ARGO-270420/599
Improper Privilege Management	08-04-2020	6.5	As of v1.5.0, the default admin password is set to the argocd-server pod name. For insiders with access to the cluster or logs, this issue could be abused for privilege escalation, as Argo has privileged roles. A malicious insider is the most realistic threat, but pod names are not meant to be kept secret and could wind up just about anywhere. **CVE ID : CVE-2020-8828**	N/A	A-LIN-ARGO-270420/600
logicaldoc					
logicaldoc					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-04-2020	5	LogicalDoc before 8.3.3 allows /servlet.gupld Directory Traversal, a different vulnerability than CVE-2020-9423 and CVE-2020-10365. **CVE ID : CVE-2020-**	N/A	A-LOG-LOGI-270420/601

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10366		
Malwarebytes					
adwcleaner					
Untrusted Search Path	06-04-2020	6.9	An Untrusted Search Path vulnerability in Malwarebytes AdwCleaner 8.0.3 could cause arbitrary code execution with SYSTEM privileges when a malicious DLL library is loaded. **CVE ID : CVE-2020-11507**	https://forums.malwarebytes.com/topic/258140-release-adwcleaner-804/	A-MAL-ADWC-270420/602
mbconnectline					
mbconnect24					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	14-04-2020	5	An issue was discovered in the MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 software in all versions through 2.5.0. There is an unauthenticated SQL injection in DATA24, allowing attackers to discover database and table names. **CVE ID : CVE-2020-10381**	https://www.mbconnectline.de/en/support/sicherheitshinweise.html	A-MBC-MBCO-270420/603
N/A	14-04-2020	7.5	An issue was discovered in the MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 software in all versions through 2.5.0. There is an authenticated remote code execution in the backup-scheduler.	https://www.mbconnectline.de/en/support/sicherheitshinweise.html	A-MBC-MBCO-270420/604

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-10382		
N/A	14-04-2020	7.5	An issue was discovered in the MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 software in all versions through 2.5.0. There is an unauthenticated remote code execution in the com_mb24sysapi module. **CVE ID : CVE-2020-10383**	https://www.mbconnectline.de/en/support/sicherheitshinweise.html	A-MBC-MBCO-270420/605
Improper Privilege Management	14-04-2020	7.2	An issue was discovered in the MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 software in all versions through 2.5.0. There is a local privilege escalation from the www-data account to the root account. **CVE ID : CVE-2020-10384**	https://www.mbconnectline.de/en/support/sicherheitshinweise.html	A-MBC-MBCO-270420/606
mymbconnect24					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	14-04-2020	5	An issue was discovered in the MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 software in all versions through 2.5.0. There is an unauthenticated SQL injection in DATA24, allowing attackers to discover database and table names. **CVE ID : CVE-2020-10381**	https://www.mbconnectline.de/en/support/sicherheitshinweise.html	A-MBC-MYMB-270420/607

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	14-04-2020	7.5	An issue was discovered in the MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 software in all versions through 2.5.0. There is an authenticated remote code execution in the backup-scheduler. **CVE ID : CVE-2020-10382**	https://www.mbconnectline.de/en/support/sicherheitshinweise.html	A-MBC-MYMB-270420/608
N/A	14-04-2020	7.5	An issue was discovered in the MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 software in all versions through 2.5.0. There is an unauthenticated remote code execution in the com_mb24sysapi module. **CVE ID : CVE-2020-10383**	https://www.mbconnectline.de/en/support/sicherheitshinweise.html	A-MBC-MYMB-270420/609
Improper Privilege Management	14-04-2020	7.2	An issue was discovered in the MB CONNECT LINE mymbCONNECT24 and mbCONNECT24 software in all versions through 2.5.0. There is a local privilege escalation from the www-data account to the root account. **CVE ID : CVE-2020-10384**	https://www.mbconnectline.de/en/support/sicherheitshinweise.html	A-MBC-MYMB-270420/610
Mcafee					
endpoint_security					
Incorrect Permission Assignment for Critical	01-04-2020	4.6	Improper access control vulnerability in ESConfigTool.exe in ENS for Windows all current	https://kc.mcafee.com/corporate/index?page	A-MCA-ENDP-270420/611

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource			versions allows a local administrator to alter the ENS configuration up to and including disabling all protection offered by ENS via insecurely implemented encryption of configuration for export and import. **CVE ID : CVE-2020-7263**	=content&id=SB10314	
media_library_assistant_project					
media_library_assistant					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-04-2020	4.3	The Media Library Assistant plugin before 2.82 for Wordpress suffers from multiple XSS vulnerabilities in all Settings/Media Library Assistant tabs, which allow remote authenticated users to execute arbitrary JavaScript. **CVE ID : CVE-2020-11731**	N/A	A-MED-MEDI-270420/612
Information Exposure	13-04-2020	5	The Media Library Assistant plugin before 2.82 for Wordpress suffers from a Local File Inclusion vulnerability in mla_gallery link=download. **CVE ID : CVE-2020-11732**	N/A	A-MED-MEDI-270420/613
Mediawiki					
mediawiki					
Improper Encoding or	03-04-2020	5	In MediaWiki before 1.34.1, users can add	https://lists.wikimedia.	A-MED-MEDI-270420/614

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Escaping of Output			various Cascading Style Sheets (CSS) classes (which can affect what content is shown or hidden in the user interface) to arbitrary DOM nodes via HTML content within a MediaWiki page. This occurs because jquery.makeCollapsible allows applying an event handler to any Cascading Style Sheets (CSS) selector. There is no known way to exploit this for cross-site scripting (XSS). **CVE ID : CVE-2020-10960**	org/pipermail/wikitech-l/2020-March/093243.html, https://phabricator.wikimedia.org/T246602	
mh-wikibot_project					
mh-wikibot					
Improper Privilege Management	07-04-2020	6.4	MH-WikiBot (an IRC Bot for interacting with the Miraheze API), had a bug that allowed any unprivileged user to access the steward commands on the IRC interface by impersonating the Nickname used by a privileged user as no check was made to see if they were logged in. The issue has been fixed in commit 23d9d5b0a59667a5d6816fdabb960b537a5f9ed1.	https://github.com/examknow/MH-WikiBot/security/advisories/GHSA-7hf3-wvp8-34r9	A-MH--MH-W-270420/615

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5302		
microstrategy					
microstrategy_web					
Information Exposure	02-04-2020	5	Microstrategy Web 10.4 exposes the JVM configuration, CPU architecture, installation folder, and other information through the URL /MicroStrategyWS/happyaxis.jsp. An attacker could use this vulnerability to learn more about the environment the application is running in. **CVE ID : CVE-2020-11450**	N/A	A-MIC-MICR-270420/616
Unrestricted Upload of File with Dangerous Type	02-04-2020	6.5	The Upload Visualization plugin in the Microstrategy Web 10.4 admin panel allows an administrator to upload a ZIP archive containing files with arbitrary extensions and data. (This is also exploitable via SSRF.) **CVE ID : CVE-2020-11451**	N/A	A-MIC-MICR-270420/617
Server-Side Request Forgery (SSRF)	02-04-2020	4	Microstrategy Web 10.4 includes functionality to allow users to import files or data from external resources such as URLs or databases. By providing an external URL under attacker control, it's possible to send requests	N/A	A-MIC-MICR-270420/618

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to external resources (aka SSRF) or leak files from the local system using the file:// stream wrapper. **CVE ID : CVE-2020-11452**		
Server-Side Request Forgery (SSRF)	02-04-2020	5	Microstrategy Web 10.4 is vulnerable to Server-Side Request Forgery in the Test Web Service functionality exposed through the path /MicroStrategyWS/. The functionality requires no authentication and, while it is not possible to pass parameters in the SSRF request, it is still possible to exploit it to conduct port scanning. An attacker could exploit this vulnerability to enumerate the resources allocated in the network (IP addresses and services exposed). **CVE ID : CVE-2020-11453**	N/A	A-MIC-MICR-270420/619
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-04-2020	3.5	Microstrategy Web 10.4 is vulnerable to Stored XSS in the HTML Container and Insert Text features in the window, allowing for the creation of a new dashboard. In order to exploit this vulnerability, a user needs to get access to a shared dashboard or have the ability to create a dashboard on the	N/A	A-MIC-MICR-270420/620

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			application. **CVE ID : CVE-2020-11454**		
Misp					
misp					
Information Exposure	02-04-2020	4	app/Model/feed.php in MISP before 2.4.124 allows administrators to choose arbitrary files that should be ingested by MISP. This does not cause a leak of the full contents of a file, but does cause a leaks of strings that match certain patterns. Among the data that can leak are passwords from database.php or GPG key passphrases from config.php. **CVE ID : CVE-2020-11458**	N/A	A-MIS-MISP-270420/621
Mongodb					
mongodb_enterprise_kubernetes_operator					
Improper Certificate Validation	09-04-2020	4	X.509 certificates generated by the MongoDB Enterprise Kubernetes Operator may allow an attacker with access to the Kubernetes cluster improper access to MongoDB instances. Customers who do not use X.509 authentication, and those who do not use the Operator to generate their X.509 certificates are unaffected.	N/A	A-MON-MONG-270420/622

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7922		
Nchsoftware					
express_invoice					
Insufficiently Protected Credentials	07-04-2020	2.1	NCH Express Invoice 7.25 allows local users to discover the cleartext password by reading the configuration file. **CVE ID : CVE-2020-11560**	N/A	A-NCH-EXPR-270420/623
Improper Privilege Management	07-04-2020	6.5	In NCH Express Invoice 7.25, an authenticated low-privilege user can enter a crafted URL to access higher-privileged functionalities such as the "Add New Item" screen. **CVE ID : CVE-2020-11561**	N/A	A-NCH-EXPR-270420/624
Netease					
pomelo-monitor					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	02-04-2020	7.5	pomelo-monitor through 0.3.7 is vulnerable to Command Injection.It allows injection of arbitrary commands as part of 'pomelo-monitor' params. **CVE ID : CVE-2020-7620**	N/A	A-NET-POME-270420/625
Netgate					
Pfsense					
Improper Neutralization of Input During Web Page Generation ('Cross-site	01-04-2020	3.5	pfSense before 2.4.5 has stored XSS in system_usermanager_add privs.php in the WebGUI via the descr parameter (aka full name) of a user.	N/A	A-NET-PFSE-270420/626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			**CVE ID : CVE-2020-11457**		
netty					
netty					
Improper Restriction of Operations within the Bounds of a Memory Buffer	07-04-2020	7.5	The ZlibDecoders in Netty 4.1.x before 4.1.46 allow for unbounded memory allocation while decoding a ZlibEncoded byte stream. An attacker could send a large ZlibEncoded byte stream to the Netty server, forcing the server to allocate all of its free memory to a single decoder. **CVE ID : CVE-2020-11612**	N/A	A-NET-NETT-270420/627
node-key-sender_project					
node-key-sender					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	02-04-2020	7.5	node-key-sender through 1.0.11 is vulnerable to Command Injection. It allows execution of arbitrary commands via the 'arrParams' argument in the 'execute()' function. **CVE ID : CVE-2020-7627**	N/A	A-NOD-NODE-270420/628
node-mpv_project					
node-mpv					
Improper Neutralization of Special Elements in Output Used by a Downstream Component	06-04-2020	7.5	node-mpv through 1.4.3 is vulnerable to Command Injection. It allows execution of arbitrary commands via the options argument. **CVE ID : CVE-2020-7632**	N/A	A-NOD-NODE-270420/629

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Injection')					
npm-programmatic_project					
npm-programmatic					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-04-2020	7.5	npm-programmatic through 0.0.12 is vulnerable to Command Injection.The packages and option properties are concatenated together without any validation and are used by the 'exec' function directly. **CVE ID : CVE-2020-7614**	N/A	A-NPM-NPM--270420/630
octech					
oempro					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-04-2020	3.5	Octech Oempro 4.7 through 4.11 allow XSS by an authenticated user. The parameter CampaignName in Campaign.Create is vulnerable. **CVE ID : CVE-2020-9460**	N/A	A-OCT-OEMP-270420/631
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-04-2020	3.5	Octech Oempro 4.7 through 4.11 allow stored XSS by an authenticated user. The FolderName parameter of the Media.CreateFolder command is vulnerable. **CVE ID : CVE-2020-9461**	N/A	A-OCT-OEMP-270420/632
oculus					
desktop					
Improper Privilege Management	08-04-2020	4.6	Writing to an unprivileged file from a privileged OVRRedir.exe process in Oculus Desktop	https://www.facebook.com/security/advisorie	A-OCU-DESK-270420/633

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 1.44.0.32849 on Windows allows local users to write to arbitrary files and consequently gain privileges via vectors involving a hard link to a log file. **CVE ID : CVE-2020-1885**	s/cve-2020-1885	
op-browser_project					
op-browser					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	02-04-2020	7.5	op-browser through 1.0.6 is vulnerable to Command Injection. It allows execution of arbitrary commands via the url function. **CVE ID : CVE-2020-7625**	N/A	A-OP--OP-B-270420/634
open_upload_project					
open_upload					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-04-2020	4.3	Open Upload through 0.4.3 allows XSS via index.php?action=u and the filename field. **CVE ID : CVE-2020-11712**	N/A	A-OPE-OPEN-270420/635
openresty					
openresty					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	12-04-2020	5	An issue was discovered in OpenResty before 1.15.8.4. ngx_http_lua_subrequest.c allows HTTP request smuggling, as demonstrated by the ngx.location.capture API. **CVE ID : CVE-2020-**	N/A	A-OPE-OPEN-270420/636

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			11724		
Opensuse					
texlive-filesystem					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-04-2020	4.4	A Race Condition Enabling Link Following vulnerability in the packaging of texlive-filesystem of SUSE Linux Enterprise Module for Desktop Applications 15-SP1, SUSE Linux Enterprise Software Development Kit 12-SP4, SUSE Linux Enterprise Software Development Kit 12-SP5; openSUSE Leap 15.1 allows local users to corrupt files or potentially escalate privileges. This issue affects: SUSE Linux Enterprise Module for Desktop Applications 15-SP1 texlive-filesystem versions prior to 2017.135-9.5.1. SUSE Linux Enterprise Software Development Kit 12-SP4 texlive-filesystem versions prior to 2013.74-16.5.1. SUSE Linux Enterprise Software Development Kit 12-SP5 texlive-filesystem versions prior to 2013.74-16.5.1. openSUSE Leap 15.1 texlive-filesystem versions prior to 2017.135-lp151.8.3.1. **CVE ID : CVE-2020-8016**	https://bugzilla.suse.com/show_bug.cgi?id=1159740	A-OPE-TEXL-270420/637

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-04-2020	3.3	A Race Condition Enabling Link Following vulnerability in the cron job shipped with texlive-filesystem of SUSE Linux Enterprise Module for Desktop Applications 15-SP1, SUSE Linux Enterprise Software Development Kit 12-SP4, SUSE Linux Enterprise Software Development Kit 12-SP5; openSUSE Leap 15.1 allows local users in group mktex to delete arbitrary files on the system This issue affects: SUSE Linux Enterprise Module for Desktop Applications 15-SP1 texlive-filesystem versions prior to 2017.135-9.5.1. SUSE Linux Enterprise Software Development Kit 12-SP4 texlive-filesystem versions prior to 2013.74-16.5.1. SUSE Linux Enterprise Software Development Kit 12-SP5 texlive-filesystem versions prior to 2013.74-16.5.1. openSUSE Leap 15.1 texlive-filesystem versions prior to 2017.135-lp151.8.3.1. **CVE ID : CVE-2020-8017**	https://bugzilla.suse.com/show_bug.cgi?id=1158910	A-OPE-TEXL-270420/638
opsramp					
gateway					
Use of Hard-	08-04-2020	10	OpsRamp Gateway 3.0.0	N/A	A-OPS-GATE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
coded Credentials			has a backdoor account vadmin with the password 9vt@f3Vt that allows root SSH access to the server. **CVE ID : CVE-2020-11543**		270420/639
ory					
hydra					
Authentication Bypass by Capture-replay	06-04-2020	3.5	In Hydra (an OAuth2 Server and OpenID Certified™ OpenID Connect Provider written in Go), before version 1.4.0+oryOS.17, when using client authentication method 'private_key_jwt' [1], OpenId specification says the following about assertion `jti`: "A unique identifier for the token, which can be used to prevent reuse of the token. These tokens MUST only be used once, unless conditions for reuse were negotiated between the parties". Hydra does not check the uniqueness of this `jti` value. Exploiting this vulnerability is somewhat difficult because: - TLS protects against MITM which makes it difficult to intercept valid tokens for replay attacks - The expiry time of the JWT gives only a short window	https://github.com/ory/hydra/security/advisories/GHSA-3p3g-vpw6-4w66	A-ORY-HYDR-270420/640

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of opportunity where it could be replayed This has been patched in version v1.4.0+oryOS.17 **CVE ID : CVE-2020-5300**		
Paessler					
prtg_network_monitor					
Information Exposure	05-04-2020	5	PRTG Network Monitor before 20.1.57.1745 allows remote unauthenticated attackers to obtain information about probes running or the server itself (CPU usage, memory, Windows version, and internal statistics) via an HTTP request, as demonstrated by type=probes to login.htm or index.htm. **CVE ID : CVE-2020-11547**	N/A	A-PAE-PRTG-270420/641
Paloaltonetworks					
traps					
Improper Privilege Management	08-04-2020	3.6	An insecure temporary file vulnerability in Palo Alto Networks Traps allows a local authenticated Windows user to escalate privileges or overwrite system files. This issue affects Palo Alto Networks Traps 5.0 versions before 5.0.8; 6.1 versions before 6.1.4 on Windows. This issue does not affect Cortex XDR 7.0. This issue does not affect	N/A	A-PAL-TRAP-270420/642

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Traps for Linux or MacOS. **CVE ID : CVE-2020-1991**		
globalprotect					
Information Exposure	08-04-2020	2.1	An information exposure vulnerability in the logging component of Palo Alto Networks Global Protect Agent allows a local authenticated user to read VPN cookie information when the troubleshooting logging level is set to "Dump". This issue affects Palo Alto Networks Global Protect Agent 5.0 versions prior to 5.0.9; 5.1 versions prior to 5.1.1. **CVE ID : CVE-2020-1987**	N/A	A-PAL-GLOB-270420/643
Unquoted Search Path or Element	08-04-2020	7.2	An unquoted search path vulnerability in the Windows release of Global Protect Agent allows an authenticated local user with file creation privileges on the root of the OS disk (C:\) or to Program Files directory to gain system privileges. This issue affects Palo Alto Networks GlobalProtect Agent 5.0 versions before 5.0.5; 4.1 versions before 4.1.13 on Windows; **CVE ID : CVE-2020-1988**	N/A	A-PAL-GLOB-270420/644
Improper Privilege Management	08-04-2020	7.2	An incorrect privilege assignment vulnerability when writing application-	N/A	A-PAL-GLOB-270420/645

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specific files in the Palo Alto Networks Global Protect Agent for Linux on ARM platform allows a local authenticated user to gain root privileges on the system. This issue affects Palo Alto Networks Global Protect Agent for Linux 5.0 versions before 5.0.8; 5.1 versions before 5.1.1. **CVE ID : CVE-2020-1989**		
vm-series					
Insufficiently Protected Credentials	08-04-2020	1.9	TechSupport files generated on Palo Alto Networks VM Series firewalls for Microsoft Azure platform configured with high availability (HA) inadvertently collect Azure dashboard service account credentials. These credentials are equivalent to the credentials associated with the Contributor role in Azure. A user with the credentials will be able to manage all the Azure resources in the subscription except for granting access to other resources. These credentials do not allow login access to the VMs themselves. This issue affects VM Series Plugin versions before 1.0.9 for	N/A	A-PAL-VM-S-270420/646

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PAN-OS 9.0. This issue does not affect VM Series in non-HA configurations or on other cloud platforms. It does not affect hardware firewall appliances. Since becoming aware of the issue, Palo Alto Networks has safely deleted all the tech support files with the credentials. We now filter and remove these credentials from all TechSupport files sent to us. The TechSupport files uploaded to Palo Alto Networks systems were only accessible by authorized personnel with valid Palo Alto Networks credentials. We do not have any evidence of malicious access or use of these credentials. **CVE ID : CVE-2020-1978**		
secdo					
Improper Input Validation	08-04-2020	7.2	Secdo tries to execute a script at a hardcoded path if present, which allows a local authenticated user with 'create folders or append data' access to the root of the OS disk (C:\) to gain system privileges if the path does not already exist or is writable. This issue affects all versions of Secdo for Windows. **CVE ID : CVE-2020-1984**	N/A	A-PAL-SECD-270420/647

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	08-04-2020	4.6	Incorrect Default Permissions on C:\Programdata\Secdo\Logs folder in Secdo allows local authenticated users to overwrite system files and gain escalated privileges. This issue affects all versions Secdo for Windows. **CVE ID : CVE-2020-1985**	N/A	A-PAL-SECD-270420/648
Improper Input Validation	08-04-2020	4.9	Improper input validation vulnerability in Secdo allows an authenticated local user with 'create folders or append data' access to the root of the OS disk (C:\) to cause a system crash on every login. This issue affects all versions Secdo for Windows. **CVE ID : CVE-2020-1986**	N/A	A-PAL-SECD-270420/649
periscopeholdings					
buyspeed					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-04-2020	3.5	Periscope BuySpeed version 14.5 is vulnerable to stored cross-site scripting, which could allow a local, authenticated attacker to store arbitrary JavaScript within the application. This JavaScript is subsequently displayed by the application without sanitization and is executed in the browser of the user, which could	N/A	A-PER-BUYS-270420/650

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			possibly cause website redirection, session hijacking, or information disclosure. This vulnerability has been patched in BuySpeed version 15.3. **CVE ID : CVE-2020-9056**		
PHP					
php					
Out-of-bounds Read	01-04-2020	5.8	In PHP versions 7.2.x below 7.2.9, 7.3.x below 7.3.16 and 7.4.x below 7.4.34, while parsing EXIF data with exif_read_data() function, it is possible for malicious data to cause PHP to read one byte of uninitialized memory. This could potentially lead to information disclosure or crash. **CVE ID : CVE-2020-7064**	https://security.netapp.com/advisory/ntap-20200403-0001/	A-PHP-PHP-270420/651
Out-of-bounds Write	01-04-2020	6.8	In PHP versions 7.3.x below 7.3.16 and 7.4.x below 7.4.34, while using mb_strtolower() function with UTF-32LE encoding, certain invalid strings could cause PHP to overwrite stack-allocated buffer. This could lead to memory corruption, crashes and potentially code execution. **CVE ID : CVE-2020-7065**	https://security.netapp.com/advisory/ntap-20200403-0001/	A-PHP-PHP-270420/652
N/A	01-04-2020	4.3	In PHP versions 7.2.x below 7.2.9, 7.3.x below 7.3.16 and 7.4.x below	https://security.netapp.com/advi	A-PHP-PHP-270420/653

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			7.4.34, while using get_headers() with user-supplied URL, if the URL contains zero (\0) character, the URL will be silently truncated at it. This may cause some software to make incorrect assumptions about the target of the get_headers() and possibly send some information to a wrong server. **CVE ID : CVE-2020-7066**	sory/ntap-20200403-0001/	
primekey					
ejbca					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-04-2020	4.3	An issue was discovered in EJBCA before 6.15.2.6 and 7.x before 7.3.1.2. Two Cross Side Scripting (XSS) vulnerabilities have been found in the Public Web and the Certificate/CRL download servlets. **CVE ID : CVE-2020-11626**	N/A	A-PRI-EJBC-270420/654
Cross-Site Request Forgery (CSRF)	08-04-2020	6.8	An issue was discovered in EJBCA before 6.15.2.6 and 7.x before 7.3.1.2. A Cross Site Request Forgery (CSRF) issue has been found in the CA UI. **CVE ID : CVE-2020-11627**	N/A	A-PRI-EJBC-270420/655
Incorrect Authorization	08-04-2020	5	An issue was discovered in EJBCA before 6.15.2.6 and 7.x before 7.3.1.2. It is	N/A	A-PRI-EJBC-270420/656

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			intended to support restriction of available remote protocols (CMP, ACME, REST, etc.) through the system configuration. These restrictions can be bypassed by modifying the URI string from a client. (EJBCA's internal access control restrictions are still in place, and each respective protocol must be configured to allow for enrollment.) **CVE ID : CVE-2020-11628**		
Unrestricted Upload of File with Dangerous Type	08-04-2020	6.5	An issue was discovered in EJBCA before 6.15.2.6 and 7.x before 7.3.1.2. The External Command Certificate Validator, which allows administrators to upload external linters to validate certificates, is supposed to save uploaded test certificates to the server. An attacker who has gained access to the CA UI could exploit this to upload malicious scripts to the server. (Risks associated with this issue alone are negligible unless a malicious user already has gained access to the CA UI through other means, as a trusted user is already trusted to upload scripts by virtue of having access to the	N/A	A-PRI-EJBC-270420/657

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validator.) **CVE ID : CVE-2020-11629**		
Deserialization of Untrusted Data	08-04-2020	7.5	An issue was discovered in EJBCA before 6.15.2.6 and 7.x before 7.3.1.2. In several sections of code, the verification of serialized objects sent between nodes (connected via the Peers protocol) allows insecure objects to be deserialized. **CVE ID : CVE-2020-11630**	N/A	A-PRI-EJBC-270420/658
Improper Input Validation	08-04-2020	4	An issue was discovered in EJBCA before 6.15.2.6 and 7.x before 7.3.1.2. An error state can be generated in the CA UI by a malicious user. This, in turn, allows exploitation of other bugs. This follow-on exploitation can lead to privilege escalation and remote code execution. (This is exploitable only when at least one accessible port lacks a requirement for client certificate authentication. These ports are 8442 or 8080 in a standard installation.) **CVE ID : CVE-2020-11631**	N/A	A-PRI-EJBC-270420/659
projectworlds					
official_car_rental_system					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	06-04-2020	6.5	An issue was discovered in Project Worlds Official Car Rental System 1. It allows the admin user to run commands on the server with their account because the upload section on the file-manager page contains an arbitrary file upload vulnerability via add_cars.php. There are no upload restrictions for executable files. **CVE ID : CVE-2020-11544**	N/A	A-PRO-OFFI-270420/660
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-04-2020	7.5	Project Worlds Official Car Rental System 1 is vulnerable to multiple SQL injection issues, as demonstrated by the email and parameters (account.php), uname and pass parameters (login.php), and id parameter (book_car.php) This allows an attacker to dump the MySQL database and to bypass the login authentication prompt. **CVE ID : CVE-2020-11545**	N/A	A-PRO-OFFI-270420/661
provideserver					
provide_ftp_server					
Cross-Site Request Forgery (CSRF)	12-04-2020	6.8	An issue was discovered in ProVide (formerly zFTPServer) through 13.1. CSRF exists in the	N/A	A-PRO-PROV-270420/662

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			User Web Interface, as demonstrated by granting filesystem access to the public for uploading and deleting files and directories. **CVE ID : CVE-2020-11701**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-04-2020	4.3	An issue was discovered in ProVide (formerly zFTPServer) through 13.1. The User Web Interface has Multiple Stored and Reflected XSS issues. Collaborate is Reflected via the filename parameter. Collaborate is Stored via the displayname parameter. Deletemultiple is Reflected via the files parameter. Share is Reflected via the target parameter. Share is Stored via the displayname parameter. Waitedit is Reflected via the Host header. **CVE ID : CVE-2020-11702**	N/A	A-PRO-PROV-270420/663
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	12-04-2020	5	An issue was discovered in ProVide (formerly zFTPServer) through 13.1. /ajax/GetInheritedProperties allows HTTP Response Splitting via the language parameter. **CVE ID : CVE-2020-**	N/A	A-PRO-PROV-270420/664

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			11703		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-04-2020	4.3	An issue was discovered in ProVide (formerly zFTPServer) through 13.1. The Admin Web Interface has Multiple Stored and Reflected XSS. GetInheritedProperties is Reflected via the groups parameter. GetUserInfo is Reflected via POST data. SetUserInfo is Stored via the general parameter. **CVE ID : CVE-2020-11704**	N/A	A-PRO-PROV-270420/665
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-04-2020	7.5	An issue was discovered in ProVide (formerly zFTPServer) through 13.1. /ajax/ImportCertificate allows an attacker to load an arbitrary certificate in .pfx format or overwrite arbitrary files via the fileName parameter. **CVE ID : CVE-2020-11705**	N/A	A-PRO-PROV-270420/666
Cross-Site Request Forgery (CSRF)	12-04-2020	6.8	An issue was discovered in ProVide (formerly zFTPServer) through 13.1. The Admin Interface allows CSRF for actions such as: Change any username and password, admin ones included; Create/Delete users; Enable/Disable Services; Set a rogue update proxy; and Shutdown the server.	N/A	A-PRO-PROV-270420/667

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-11706		
Improper Input Validation	12-04-2020	6.5	An issue was discovered in ProVide (formerly zFTPServer) through 13.1. It doesn't enforce permission over Windows Symlinks or Junctions. As a result, a low-privileged user (non-admin) can craft a Junction Link in a directory he has full control of, breaking out of the sandbox. **CVE ID : CVE-2020-11707**	N/A	A-PRO-PROV-270420/668
Improper Privilege Management	12-04-2020	7.5	An issue was discovered in ProVide (formerly zFTPServer) through 13.1. Privilege escalation can occur via the /ajax/SetUserInfo messages parameter because of the EXECUTE() feature, which is for executing programs when certain events are triggered. **CVE ID : CVE-2020-11708**	N/A	A-PRO-PROV-270420/669
Pulsesecure					
pulse_connect_secure					
Improper Certificate Validation	06-04-2020	6.4	An issue was discovered in Pulse Secure Pulse Connect Secure (PCS) through 2020-04-06. The applet in tncc.jar, executed on macOS, Linux, and Solaris clients	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44426	A-PUL-PULS-270420/670

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			when a Host Checker policy is enforced, accepts an arbitrary SSL certificate. **CVE ID : CVE-2020-11580**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-04-2020	9.3	An issue was discovered in Pulse Secure Pulse Connect Secure (PCS) through 2020-04-06. The applet in tncc.jar, executed on macOS, Linux, and Solaris clients when a Host Checker policy is enforced, allows a man-in-the-middle attacker to perform OS command injection attacks (against a client) via shell metacharacters to the doCustomRemediateInstructions method, because Runtime.getRuntime().exec() is used. **CVE ID : CVE-2020-11581**	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44426	A-PUL-PULS-270420/671
Improper Restriction of Excessive Authentication Attempts	06-04-2020	3.3	An issue was discovered in Pulse Secure Pulse Connect Secure (PCS) through 2020-04-06. The applet in tncc.jar, executed on macOS, Linux, and Solaris clients when a Host Checker policy is enforced, launches a TCP server that accepts local connections on a random port. This can be reached	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44426	A-PUL-PULS-270420/672

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			by local HTTP clients, because up to 25 invalid lines are ignored, and because DNS rebinding can occur. (This server accepts, for example, a setcookie command that might be relevant to CVE-2020-11581 exploitation.) **CVE ID : CVE-2020-11582**		
Qemu					
qemu					
Out-of-bounds Write	06-04-2020	6.8	hw/net/tulip.c in QEMU 4.2.0 has a buffer overflow during the copying of tx/rx buffers because the frame size is not validated against the r/w data length. **CVE ID : CVE-2020-11102**	N/A	A-QEM-QEMU-270420/673
rankmath					
rankmath					
Improper Privilege Management	07-04-2020	7.5	The Rank Math plugin through 1.0.40.2 for WordPress allows unauthenticated remote attackers to update arbitrary WordPress metadata, including the ability to escalate or revoke administrative privileges for existing users via the unsecured rankmath/v1/updateMeta REST API endpoint.	N/A	A-RAN-RANK-270420/674

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-11514		
URL Redirection to Untrusted Site ('Open Redirect')	07-04-2020	5.8	The Rank Math plugin through 1.0.40.2 for WordPress allows unauthenticated remote attackers to create new URIs (that redirect to an external web site) via the unsecured rankmath/v1/updateRedirection REST API endpoint. In other words, this is not an "Open Redirect" issue; instead, it allows the attacker to create a new URI with an arbitrary name (e.g., the /exampleredirect URI). **CVE ID : CVE-2020-11515**	N/A	A-RAN-RANK-270420/675
Redhat					
keycloak					
Improper Restriction of Rendered UI Layers or Frames	06-04-2020	5.8	A vulnerability was found in all versions of Keycloak where, the pages on the Admin Console area of the application are completely missing general HTTP security headers in HTTP-responses. This does not directly lead to a security issue, yet it might aid attackers in their efforts to exploit other problems. The flaws unnecessarily make the servers more prone to Clickjacking, channel downgrade	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1728	A-RED-KEYC-270420/676

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks and other similar client-based attack vectors. **CVE ID : CVE-2020-1728**		
openshift_container_platform					
Out-of-bounds Write	02-04-2020	6.5	In hpack_dht_insert in hpack-tbl.c in the HPACK decoder in HAProxy 1.8 through 2.x before 2.1.4, a remote attacker can write arbitrary bytes around a certain location on the heap via a crafted HTTP/2 request, possibly causing remote code execution. **CVE ID : CVE-2020-11100**	https://bugzilla.redhat.com/show_bug.cgi?id=1819111, https://bugzilla.suse.com/show_bug.cgi?id=1168023, https://git.haproxy.org/?p=haproxy.git;a=commit;h=5dfc5d5cd0d2128d77253ead3acf03a421ab5b88, https://www.haproxy.org/download/2.1/src/CHANGELOG	A-RED-OPEN-270420/677
openstack					
Use of Insufficiently Random Values	13-04-2020	5.8	A vulnerability was found in Red Hat Ceph Storage 4 and Red Hat Openshift Container Storage 4.2 where, A nonce reuse vulnerability was discovered in the secure mode of the messenger v2 protocol, which can allow an attacker to forge auth	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1759	A-RED-OPEN-270420/678

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			tags and potentially manipulate the data by leveraging the reuse of a nonce in a session. Messages encrypted using a reused nonce value are susceptible to serious confidentiality and integrity attacks. **CVE ID : CVE-2020-1759**		
openshift					
Use of Insufficiently Random Values	13-04-2020	5.8	A vulnerability was found in Red Hat Ceph Storage 4 and Red Hat Openshift Container Storage 4.2 where, A nonce reuse vulnerability was discovered in the secure mode of the messenger v2 protocol, which can allow an attacker to forge auth tags and potentially manipulate the data by leveraging the reuse of a nonce in a session. Messages encrypted using a reused nonce value are susceptible to serious confidentiality and integrity attacks. **CVE ID : CVE-2020-1759**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1759	A-RED-OPEN-270420/679
ceph_storage					
Use of Insufficiently Random Values	13-04-2020	5.8	A vulnerability was found in Red Hat Ceph Storage 4 and Red Hat Openshift Container Storage 4.2 where, A nonce reuse vulnerability was discovered in the secure	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1759	A-RED-CEPH-270420/680

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mode of the messenger v2 protocol, which can allow an attacker to forge auth tags and potentially manipulate the data by leveraging the reuse of a nonce in a session. Messages encrypted using a reused nonce value are susceptible to serious confidentiality and integrity attacks. **CVE ID : CVE-2020-1759**		
Revive-adserver					
revive_adserver					
Incorrect Authorization	03-04-2020	4.6	A security restriction bypass vulnerability has been discovered in Revive Adserver version < 5.0.5 by HackerOne user hoangn144. Revive Adserver, like many other applications, requires the logged in user to type the current password in order to change the e-mail address or the password. It was however possible for anyone with access to a Revive Adserver admin user interface to bypass such check and change e-email address or password of the currently logged in user by altering the form payload.The attack requires physical access to the user interface of a logged in user. If the POST payload	N/A	A-REV-REVI-270420/681

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			was altered by turning the "pwold" parameter into an array, Revive Adserver would fetch and authorise the operation even if no password was provided. **CVE ID : CVE-2020-8142**		
URL Redirection to Untrusted Site ('Open Redirect')	03-04-2020	5.8	An Open Redirect vulnerability was discovered in Revive Adserver version < 5.0.5 and reported by HackerOne user hoangn144. A remote attacker could trick logged-in users to open a specifically crafted link and have them redirected to any destination.The CSRF protection of the "/www/admin/*-modify.php" could be skipped if no meaningful parameter was sent. No action was performed, but the user was still redirected to the target page, specified via the "returnurl" GET parameter. **CVE ID : CVE-2020-8143**	N/A	A-REV-REVI-270420/682
Rockwellautomation					
rslinx_classic					
Incorrect Permission Assignment for Critical Resource	13-04-2020	7.2	In Rockwell Automation RSLinx Classic versions 4.1.00 and prior, an authenticated local attacker could modify a registry key, which could	N/A	A-ROC-RSLI-270420/683

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to the execution of malicious code using system privileges when opening RSLinx Classic. **CVE ID : CVE-2020-10642**		
sds_project					
sds					
Improper Input Validation	07-04-2020	5	sds through 3.2.0 is vulnerable to Prototype Pollution.The library could be tricked into adding or modifying properties of the 'Object.prototype' by abusing the 'set' function located in 'js/set.js'. **CVE ID : CVE-2020-7618**	N/A	A-SDS-SDS-270420/684
search_meter_project					
search_meter					
Improper Input Validation	05-04-2020	7.5	The Search Meter plugin through 2.13.2 for WordPress allows user input introduced in the search bar to be any formula. The attacker could achieve remote code execution via CSV injection if a wp-admin/index.php?page=search-meter Export is performed. **CVE ID : CVE-2020-11548**	N/A	A-SEA-SEAR-270420/685
slack					
nebula					
Improper	02-04-2020	8.5	Slack Nebula through	N/A	A-SLA-NEBU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Limitation of a Pathname to a Restricted Directory ('Path Traversal')			1.1.0 contains a relative path vulnerability that allows a low-privileged attacker to execute code in the context of the root user via tun_darwin.go or tun_windows.go. A user can also use Nebula to execute arbitrary code in the user's own context, e.g., for user-level persistence or to bypass security controls. NOTE: the vendor states that this "requires a high degree of access and other preconditions that are tough to achieve." **CVE ID : CVE-2020-11498**		270420/686
snapcreek					
duplicator					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	13-04-2020	5	The Snap Creek Duplicator plugin before 1.3.28 for WordPress (and Duplicator Pro before 3.8.7.1) allows Directory Traversal via ../ in the file parameter to duplicator_download or duplicator_init. **CVE ID : CVE-2020-11738**	N/A	A-SNA-DUPL-270420/687
Solarwinds					
dameware					
Buffer Copy without Checking Size of Input	07-04-2020	4.3	Classic buffer overflow in SolarWinds Dameware allows a remote, unauthenticated attacker	N/A	A-SOL-DAME-270420/688

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			to cause a denial of service by sending a large 'SigPubkeyLen' during ECDH key exchange. **CVE ID : CVE-2020-5734**		
Sonatype					
nexus					
Missing Authorization	01-04-2020	9	Sonatype Nexus Repository before 3.21.2 allows JavaEL Injection (issue 1 of 2). **CVE ID : CVE-2020-10199**	https://support.sonatype.com/hc/en-us/articles/360044882533	A-SON-NEXU-270420/689
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-04-2020	3.5	Sonatype Nexus Repository before 3.21.2 allows XSS. **CVE ID : CVE-2020-10203**	https://support.sonatype.com/hc/en-us/articles/360044361594	A-SON-NEXU-270420/690
Missing Authorization	01-04-2020	9	Sonatype Nexus Repository before 3.21.2 allows Remote Code Execution. **CVE ID : CVE-2020-10204**	https://support.sonatype.com/hc/en-us/articles/360044882533	A-SON-NEXU-270420/691
Incorrect Default Permissions	02-04-2020	6.5	Sonatype Nexus Repository Manager 3.x up to and including 3.21.2 has Incorrect Access Control. **CVE ID : CVE-2020-11444**	https://support.sonatype.com/hc/en-us/articles/360046133553	A-SON-NEXU-270420/692
Sqlite					
sqlite					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	09-04-2020	5	SQLite through 3.31.1 allows attackers to cause a denial of service (segmentation fault) via a malformed window-function query because the AggInfo object's initialization is mishandled. **CVE ID : CVE-2020-11655**	N/A	A-SQL-SQLI-270420/693
Use After Free	09-04-2020	7.5	In SQLite through 3.31.1, the ALTER TABLE implementation has a use-after-free, as demonstrated by an ORDER BY clause that belongs to a compound SELECT statement. **CVE ID : CVE-2020-11656**	N/A	A-SQL-SQLI-270420/694
starface					
unified_communication_\&_collaboration_client					
Uncontrolled Search Path Element	02-04-2020	10	STARFACE UCC Client before 6.7.1.204 on WIndows allows binary planting to execute code with System rights, aka usd-2020-0006. **CVE ID : CVE-2020-10515**	https://support.starface.de/forum/showthread.php?7916-UCC-Client-f%FCr-Windows-Version-6-7-1-204-Released-26-03-2020&p=47548	A-STA-UNIF-270420/695
Symantec					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
data_center_security					
Improper Privilege Management	06-04-2020	4.6	Symantec Data Center Security Manager Component, prior to 6.8.2 (aka 6.8 MP2), may be susceptible to a privilege escalation vulnerability, which is a type of issue whereby an attacker may attempt to compromise the software application to gain elevated access to resources that are normally protected from an application or user. **CVE ID : CVE-2020-5832**	N/A	A-SYM-DATA-270420/696
Tencent					
qqbrowser					
Improper Privilege Management	09-04-2020	7.2	QQBrowser before 10.5.3870.400 installs a Windows service TsService.exe. This file is writable by anyone belonging to the NT AUTHORITY\Authenticated Users group, which includes all local and remote users. This can be abused by local attackers to escalate privileges to NT AUTHORITY\SYSTEM by writing a malicious executable to the location of TsService. **CVE ID : CVE-2020-10551**	N/A	A-TEN-QQBR-270420/697
tendermint					
tendermint					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	10-04-2020	4.3	Tendermint before versions 0.33.3, 0.32.10, and 0.31.12 has a denial-of-service vulnerability. Tendermint does not limit the number of P2P connection requests. For each p2p connection, it allocates XXX bytes. Even though this memory is garbage collected once the connection is terminated (due to duplicate IP or reaching a maximum number of inbound peers), temporary memory spikes can lead to OOM (Out-Of-Memory) exceptions. Additionally, Tendermint does not reclaim `activeID` of a peer after it's removed in Mempool reactor. This does not happen all the time. It only happens when a connection fails (for any reason) before the Peer is created and added to all reactors. RemovePeer is therefore called before `AddPeer`, which leads to always growing memory (`activeIDs` map). The activeIDs map has a maximum size of 65535 and the node will panic if this map reaches the maximum. An attacker can create a lot of	https://github.com/tendermint/tendermint/security/advisories/GHSA-v24h-pjjv-mcp6	A-TEN-TEND-270420/698

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			connection attempts (exploiting above denial of service), which ultimately will lead to the node panicking. These issues are patched in Tendermint 0.33.3 and 0.32.10. ### For more information If you have any questions or comments about this advisory: * Open an issue in tendermint/tendermint * Email us at security@tendermint.com More information can be found here. ### Credits - Ethan Buchman (@ebuchman) for writing a test case for Denial of Service 2 and Tess Rinearson (@tessr) for fixing it - Anton Kaliaev (@melekes) for fixing Denial of Service 1 **CVE ID : CVE-2020-5303**		
Testlink					
testlink					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-04-2020	7.5	A SQL injection vulnerability in TestLink 1.9.20 allows attackers to execute arbitrary SQL commands in dragdroptreenodes.php via the node_id parameter. **CVE ID : CVE-2020-8637**	https://github.com/TestLinkOpenSourceTRMS/testlink-code/commit/d99bd8277d384f3417e917ce20bef5d061110343	A-TES-TEST-270420/699

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-04-2020	7.5	A SQL injection vulnerability in TestLink 1.9.20 allows attackers to execute arbitrary SQL commands in planUrgency.php via the urgency parameter. **CVE ID : CVE-2020-8638**	https://github.com/TestLinkOpenSourceTRMS/testlink-code/commit/58f3cc03d5f81cd5cc2ad8c7ba645cc486cebc05	A-TES-TEST-270420/700
Unrestricted Upload of File with Dangerous Type	03-04-2020	6.5	An unrestricted file upload vulnerability in keywordsImport.php in TestLink 1.9.20 allows remote attackers to execute arbitrary code by uploading a file with an executable extension. This allows an authenticated attacker to upload a malicious file (containing PHP code to execute operating system commands) to a publicly accessible directory of the application. **CVE ID : CVE-2020-8639**	https://github.com/TestLinkOpenSourceTRMS/testlink-code/commit/57d81ae350d569c5c95087997fe051c49e14516d	A-TES-TEST-270420/701
Tiki					
tikiwiki_cms\/groupware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-04-2020	4.3	There is an Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in php webpages of Tiki-Wiki Groupware. Tiki-Wiki CMS all versions through 20.0 allows malicious users to cause the	https://sourceforge.net/p/tikiwiki/code/75455, https://www.incibe-cert.es/en/early-warning/se	A-TIK-TIKI-270420/702

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			injection of malicious code fragments (scripts) into a legitimate web page. **CVE ID : CVE-2020-8966**	curity-advisories/cross-site-scripting-xss-flaws-found-tiki-wiki-cms-software	
total-soft					
responsive_poll					
Improper Authentication	13-04-2020	7.5	An issue was discovered in the Responsive Poll through 1.3.4 for Wordpress. It allows an unauthenticated user to manipulate polls, e.g., delete, clone, or view a hidden poll. This is due to the usage of the callback wp_ajax_nopriv function in Includes/Total-Soft-Poll-Ajax.php for sensitive operations. **CVE ID : CVE-2020-11673**	N/A	A-TOT-RESP-270420/703
ui					
unifi_video					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-04-2020	5.2	The UniFi Video Server v3.9.3 and prior (for Windows 7/8/10 x64) web interface Firmware Update functionality, under certain circumstances, does not validate firmware download destinations to ensure they are within the intended destination directory tree. It accepts a	https://community.ui.com/releases/Security-advisory-bulletin-006-006/3cf6264e-e0e6-4e26-a331-1d271f84673e	A-UI-UNIF-270420/704

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request with a URL to firmware update information. If the version field contains ..\ character sequences, the destination file path to save the firmware can be manipulated to be outside the intended destination directory tree. Fixed in UniFi Video Controller v3.10.3 and newer. **CVE ID : CVE-2020-8144**		
Improper Privilege Management	01-04-2020	4	The UniFi Video Server (Windows) web interface configuration restore functionality at the "backup" and "wizard" endpoints does not implement sufficient privilege checks. Low privileged users, belonging to the PUBLIC_GROUP or CUSTOM_GROUP groups, can access these endpoints and overwrite the current application configuration. This can be abused for various purposes, including adding new administrative users. Affected Products: UniFi Video Controller v3.9.3 (for Windows 7/8/10 x64) and prior. Fixed in UniFi Video Controller v3.9.6 and newer. **CVE ID : CVE-2020-8145**	https://community.ui.com/releases/Security-advisory-bulletin-006-006/3cf6264e-e0e6-4e26-a331-1d271f84673e	A-UI-UNIF-270420/705

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	01-04-2020	6.9	In UniFi Video v3.10.1 (for Windows 7/8/10 x64) there is a Local Privileges Escalation to SYSTEM from arbitrary file deletion and DLL hijack vulnerabilities. The issue was fixed by adjusting the .tsExport folder when the controller is running on Windows and adjusting the SafeDllSearchMode in the windows registry when installing UniFi-Video controller. Affected Products: UniFi Video Controller v3.10.2 (for Windows 7/8/10 x64) and prior. Fixed in UniFi Video Controller v3.10.3 and newer. **CVE ID : CVE-2020-8146**	https://community.ui.com/releases/Security-advisory-bulletin-006-006/3cf6264e-e0e6-4e26-a331-1d271f84673e	A-UI-UNIF-270420/706
universal-robots					
ur_software					
Information Exposure	06-04-2020	5.8	CB3 SW Version 3.3 and upwards, e-series SW Version 5.0 and upwards allow authenticated access to the RTDE (Real-Time Data Exchange) interface on port 30004 which allows setting registers, the speed slider fraction as well as digital and analog Outputs. Additionally unautheticated reading of robot data is also possible **CVE ID : CVE-2020-**	https://www.universal-robots.com/how-tos-and-faqs/how-to/ur-how-tos/real-time-data-exchange-rtde-guide/	A-UNI-UR_S-270420/707

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10264		
Missing Authentication for Critical Function	06-04-2020	9	Universal Robots Robot Controllers Version CB2 SW Version 1.4 upwards, CB3 SW Version 3.0 and upwards, e-series SW Version 5.0 and upwards expose a service called DashBoard server at port 29999 that allows for control over core robot functions like starting/stopping programs, shutdown, reset safety and more. The DashBoard server is not protected by any kind of authentication or authorization. **CVE ID : CVE-2020-10265**	https://www.universal-robots.com/how-tos-and-faqs/how-to/ur-how-tos/real-time-data-exchange-rtde-guide/	A-UNI-UR_S-270420/708
Missing Encryption of Sensitive Data	06-04-2020	5	Universal Robots control box CB 3.1 across firmware versions (tested on 1.12.1, 1.12, 1.11 and 1.10) does not encrypt or protect in any way the intellectual property artifacts installed from the UR+ platform of hardware and software components (URCaps). These files (*.urcaps) are stored under '/root/.urcaps' as plain zip files containing all the logic to add functionality to the UR3, UR5 and UR10 robots. This flaw allows attackers with access to	https://github.com/aliasrobotics/RVD/issues/1489	A-UNI-UR_S-270420/709

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the robot or the robot network (while in combination with other flaws) to retrieve and easily exfiltrate all installed intellectual property. **CVE ID : CVE-2020-10267**		
ur\+					
Insufficient Verification of Data Authenticity	06-04-2020	6.8	UR+ (Universal Robots+) is a platform of hardware and software component sellers, for Universal Robots robots. When installing any of these components in the robots (e.g. in the UR10), no integrity checks are performed. Moreover, the SDK for making such components can be easily obtained from Universal Robots. An attacker could exploit this flaw by crafting a custom component with the SDK, performing Person-In-The-Middle attacks (PITM) and shipping the maliciously-crafted component on demand. **CVE ID : CVE-2020-10266**	https://github.com/aliasrobotics/RVD/issues/1487	A-UNI-UR\+-270420/710
utils-extend_project					
utils-extend					
Improper Input Validation	03-04-2020	7.5	Flaw in input validation in npm package utils-extend version 1.0.8 and earlier	N/A	A-UTI-UTIL-270420/711

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may allow prototype pollution attack that may result in remote code execution or denial of service of applications using utils-extend. **CVE ID : CVE-2020-8147**		
Varnish-cache					
varnish_cache					
Improper Input Validation	08-04-2020	5	An issue was discovered in Varnish Cache before 6.0.6 LTS, 6.1.x and 6.2.x before 6.2.3, and 6.3.x before 6.3.2. It occurs when communication with a TLS termination proxy uses PROXY version 2. There can be an assertion failure and daemon restart, which causes a performance loss. **CVE ID : CVE-2020-11653**	N/A	A-VAR-VARN-270420/712
Viewvc					
viewvc					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-04-2020	2.1	ViewVC before versions 1.1.28 and 1.2.1 has a XSS vulnerability in CVS show_subdir_lastmod support. The impact of this vulnerability is mitigated by the need for an attacker to have commit privileges to a CVS repository exposed by an otherwise trusted ViewVC instance that also has the	https://github.com/viewvc/viewvc/security/advisories/GHSA-xpxf-fvqv-7mfg	A-VIE-VIEW-270420/713

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			`show_subdir_lastmod` feature enabled. The attack vector involves files with unsafe names (names that, when embedded into an HTML stream, would cause the browser to run unwanted code), which themselves can be challenging to create. This vulnerability is patched in versions 1.2.1 and 1.1.28. **CVE ID : CVE-2020-5283**		
visam					
vbase_editor					
Insecure Storage of Sensitive Information	03-04-2020	5	VISAM VBASE Editor version 11.5.0.2 and VBASE Web-Remote Module may allow an unauthenticated attacker to discover the cryptographic key from the web server and gain information about the login and the encryption/decryption mechanism, which may be exploited to bypass authentication of the HTML5 HMI web interface. **CVE ID : CVE-2020-7000**	N/A	A-VIS-VBAS-270420/714
Incorrect Default Permissions	03-04-2020	7.2	VISAM VBASE Editor version 11.5.0.2 and VBASE Web-Remote Module may allow weak or insecure permissions on the VBASE directory	N/A	A-VIS-VBAS-270420/715

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resulting in elevation of privileges or malicious effects on the system the next time a privileged user runs the application. **CVE ID : CVE-2020-7004**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-04-2020	5	VISAM VBASE Editor version 11.5.0.2 and VBASE Web-Remote Module may allow input passed in the URL that is not properly verified before use, which may allow an attacker to read arbitrary files from local resources. **CVE ID : CVE-2020-7008**	N/A	A-VIS-VBAS-270420/716
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-04-2020	7.5	VISAM VBASE Editor version 11.5.0.2 and VBASE Web-Remote Module may allow a vulnerable ActiveX component to be exploited resulting in a buffer overflow, which may lead to a denial-of-service condition and execution of arbitrary code. **CVE ID : CVE-2020-10599**	N/A	A-VIS-VBAS-270420/717
Inadequate Encryption Strength	03-04-2020	4.6	VISAM VBASE Editor version 11.5.0.2 and VBASE Web-Remote Module allow weak hashing algorithm and insecure permissions which may allow a local attacker to bypass the	N/A	A-VIS-VBAS-270420/718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			password-protected mechanism through brute-force attacks, cracking techniques, or overwriting the password hash. **CVE ID : CVE-2020-10601**		
vbase_web-remote					
Insecure Storage of Sensitive Information	03-04-2020	5	VISAM VBASE Editor version 11.5.0.2 and VBASE Web-Remote Module may allow an unauthenticated attacker to discover the cryptographic key from the web server and gain information about the login and the encryption/decryption mechanism, which may be exploited to bypass authentication of the HTML5 HMI web interface. **CVE ID : CVE-2020-7000**	N/A	A-VIS-VBAS-270420/719
Incorrect Default Permissions	03-04-2020	7.2	VISAM VBASE Editor version 11.5.0.2 and VBASE Web-Remote Module may allow weak or insecure permissions on the VBASE directory resulting in elevation of privileges or malicious effects on the system the next time a privileged user runs the application. **CVE ID : CVE-2020-7004**	N/A	A-VIS-VBAS-270420/720
Improper	03-04-2020	5	VISAM VBASE Editor	N/A	A-VIS-VBAS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Limitation of a Pathname to a Restricted Directory ('Path Traversal')			version 11.5.0.2 and VBASE Web-Remote Module may allow input passed in the URL that is not properly verified before use, which may allow an attacker to read arbitrary files from local resources. **CVE ID : CVE-2020-7008**		270420/721
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-04-2020	7.5	VISAM VBASE Editor version 11.5.0.2 and VBASE Web-Remote Module may allow a vulnerable ActiveX component to be exploited resulting in a buffer overflow, which may lead to a denial-of-service condition and execution of arbitrary code. **CVE ID : CVE-2020-10599**	N/A	A-VIS-VBAS-270420/722
Inadequate Encryption Strength	03-04-2020	4.6	VISAM VBASE Editor version 11.5.0.2 and VBASE Web-Remote Module allow weak hashing algorithm and insecure permissions which may allow a local attacker to bypass the password-protected mechanism through brute-force attacks, cracking techniques, or overwriting the password hash. **CVE ID : CVE-2020-**	N/A	A-VIS-VBAS-270420/723

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10601		
Vmware					
vcenter_server					
Incorrect Authorization	10-04-2020	6.8	Under certain conditions, vmdir that ships with VMware vCenter Server, as part of an embedded or external Platform Services Controller (PSC), does not correctly implement access controls. **CVE ID : CVE-2020-3952**	N/A	A-VMW-VCEN-270420/724
tanzu_application_service_for_vms					
Insufficiently Protected Credentials	10-04-2020	4	VMware Tanzu Application Service for VMs, 2.6.x versions prior to 2.6.18, 2.7.x versions prior to 2.7.11, and 2.8.x versions prior to 2.8.5, includes a version of PCF Autoscaling that writes database connection properties to its log, including database username and password. A malicious user with access to those logs may gain unauthorized access to the database being used by Autoscaling. **CVE ID : CVE-2020-5406**	https://tanzu.vmware.com/security/cve-2020-5406	A-VMW-TANZ-270420/725
Wireshark					
wireshark					
Improper Neutralization of Special Elements in Output Used by	10-04-2020	5	In Wireshark 3.2.0 to 3.2.2, 3.0.0 to 3.0.9, and 2.6.0 to 2.6.15, the BACapp dissector could crash. This was addressed	N/A	A-WIR-WIRE-270420/726

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Downstream Component ('Injection')			in epan/dissectors/packet-bacapp.c by limiting the amount of recursion. **CVE ID : CVE-2020-11647**		
Wolfssl					
wolfssl					
Use of a Broken or Risky Cryptographic Algorithm	12-04-2020	5	wolfSSL 4.3.0 has mulmod code in wc_ecc_mulmod_ex in ecc.c that does not properly resist timing side-channel attacks. **CVE ID : CVE-2020-11713**	N/A	A-WOL-WOLF-270420/727
wowza					
streaming_engine					
Incorrect Authorization	14-04-2020	9	A remote authenticated authorization-bypass vulnerability in Wowza Streaming Engine 4.7.8 (build 20191105123929) allows any read-only user to issue requests to the administration panel in order to change functionality. For example, a read-only user may activate the Java JMX port in unauthenticated mode and execute OS commands under root privileges. **CVE ID : CVE-2020-9004**	N/A	A-WOW-STRE-270420/728
wpleadplus					
wp_lead_plus_x					

CVSS Scoring Scale	0-1	1-2	2-3	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')	07-04-2020	3.5	An XSS vulnerability in the WP Lead Plus X plugin through 0.98 for WordPress allows logged-in users with minimal permissions to create or replace existing pages with a malicious page containing arbitrary JavaScript via the wp_ajax_core37_lp_save_page (aka core37_lp_save_page) AJAX action. **CVE ID : CVE-2020-11508**	N/A	A-WPL-WP_L-270420/729
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-04-2020	4.3	An XSS vulnerability in the WP Lead Plus X plugin through 0.98 for WordPress allows remote attackers to upload page templates containing arbitrary JavaScript via the c37_wpl_import_template admin-post action (which will execute in an administrator's browser if the template is used to create a page). **CVE ID : CVE-2020-11509**	N/A	A-WPL-WP_L-270420/730
zevenet					
zen_load_balancer					
Improper Neutralization of Special Elements used in an OS	02-04-2020	9	Manage::Certificates in Zen Load Balancer 3.10.1 allows remote authenticated admins to execute arbitrary OS	N/A	A-ZEV-ZEN_-270420/731

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			commands via shell metacharacters in the index.cgi cert_issuer, cert_division, cert_organization, cert_locality, cert_state, cert_country, or cert_email parameter. **CVE ID : CVE-2020-11490**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-04-2020	4	Monitoring::Logs in Zen Load Balancer 3.10.1 allows remote authenticated admins to conduct absolute path traversal attacks, as demonstrated by a filelog=/etc/shadow request to index.cgi. **CVE ID : CVE-2020-11491**	N/A	A-ZEV-ZEN_-270420/732
Zohocorp					
manageengine_opmanager					
Information Exposure	04-04-2020	5	In Zoho ManageEngine OpManager before 12.4.181, an unauthenticated remote attacker can send a specially crafted URI to read arbitrary files. **CVE ID : CVE-2020-11527**	N/A	A-ZOH-MANA-270420/733
manageengine_adselfservice_plus					
N/A	04-04-2020	7.5	Zoho ManageEngine ADSelfService Plus before 5815 allows unauthenticated remote code execution.	N/A	A-ZOH-MANA-270420/734

CVSS Scoring Scale	0-1	1-2	2-3	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-2020-11518		
Zoom					
meetings					
Improper Privilege Management	01-04-2020	7.2	Zoom Client for Meetings through 4.6.8 on macOS copies runwithroot to a user-writable temporary directory during installation, which allows a local process (with the user's privileges) to obtain root access by replacing runwithroot. **CVE ID : CVE-2020-11469**	N/A	A-ZOO-MEET-270420/735
Missing Authorization	01-04-2020	2.1	Zoom Client for Meetings through 4.6.8 on macOS has the disable-library-validation entitlement, which allows a local process (with the user's privileges) to obtain unprompted microphone and camera access by loading a crafted library and thereby inheriting Zoom Client's microphone and camera access. **CVE ID : CVE-2020-11470**	N/A	A-ZOO-MEET-270420/736
Use of a Broken or Risky Cryptographic Algorithm	03-04-2020	5	Zoom Client for Meetings through 4.6.9 uses the ECB mode of AES for video and audio encryption. Within a meeting, all participants use a single 128-bit key. **CVE ID : CVE-2020-**	N/A	A-ZOO-MEET-270420/737

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			11500		
Hardware					
amcrest					
1080-lite_8ch					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	H-AMC-1080-270420/738
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**	N/A	H-AMC-1080-270420/739
amdv10814-h5					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	H-AMC-AMDV-270420/740
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote	N/A	H-AMC-AMDV-270420/741

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**		
ipm-721					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	H-AMC-IPM--270420/742
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**	N/A	H-AMC-IPM--270420/743
ip2m-841					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	H-AMC-IP2M-270420/744
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote	N/A	H-AMC-IP2M-270420/745

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**		
ip2m-841-v3					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	H-AMC-IP2M-270420/746
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**	N/A	H-AMC-IP2M-270420/747
ip2m-853ew					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	H-AMC-IP2M-270420/748
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote	N/A	H-AMC-IP2M-270420/749

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**		
ip2m-858w					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	H-AMC-IP2M-270420/750
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**	N/A	H-AMC-IP2M-270420/751
ip2m-866w					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	H-AMC-IP2M-270420/752
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote	N/A	H-AMC-IP2M-270420/753

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**		
ip2m-866ew					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	H-AMC-IP2M-270420/754
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**	N/A	H-AMC-IP2M-270420/755
ip4m-1053ew					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	H-AMC-IP4M-270420/756
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote	N/A	H-AMC-IP4M-270420/757

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**		
ip8m-2454ew					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	H-AMC-IP8M-270420/758
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**	N/A	H-AMC-IP8M-270420/759
ip8m-2493eb					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	H-AMC-IP8M-270420/760
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote	N/A	H-AMC-IP8M-270420/761

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**		
ip8m-2496eb					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	H-AMC-IP8M-270420/762
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**	N/A	H-AMC-IP8M-270420/763
ip8m-2597e					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	H-AMC-IP8M-270420/764
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote	N/A	H-AMC-IP8M-270420/765

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**		
ip8m-mb2546ew					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	H-AMC-IP8M-270420/766
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**	N/A	H-AMC-IP8M-270420/767
ip8m-mt2544ew					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	H-AMC-IP8M-270420/768
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote	N/A	H-AMC-IP8M-270420/769

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**		
ip8m-t2499ew					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	H-AMC-IP8M-270420/770
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**	N/A	H-AMC-IP8M-270420/771
ipm-hx1					
Out-of-bounds Write	08-04-2020	8	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attacker can abuse this issue to crash the device and possibly execute arbitrary code. **CVE ID : CVE-2020-5735**	N/A	H-AMC-IPM--270420/772
NULL Pointer Dereference	08-04-2020	6.8	Amcrest cameras and NVR are vulnerable to a null pointer dereference over port 37777. An authenticated remote	N/A	H-AMC-IPM--270420/773

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker can abuse this issue to crash the device. **CVE ID : CVE-2020-5736**		
BD					
pyxis_medstation_es					
Information Exposure	01-04-2020	3.6	In BD Pyxis MedStation ES System v1.6.1 and Pyxis Anesthesia (PAS) ES System v1.6.1, a restricted desktop environment escape vulnerability exists in the kiosk mode functionality of affected devices. Specially crafted inputs could allow the user to escape the restricted environment, resulting in access to sensitive data. **CVE ID : CVE-2020-10598**	N/A	H-BD-PYXI-270420/774
pyxis_anesthesia_station_es					
Information Exposure	01-04-2020	3.6	In BD Pyxis MedStation ES System v1.6.1 and Pyxis Anesthesia (PAS) ES System v1.6.1, a restricted desktop environment escape vulnerability exists in the kiosk mode functionality of affected devices. Specially crafted inputs could allow the user to escape the restricted environment, resulting in access to sensitive data. **CVE ID : CVE-2020-10598**	N/A	H-BD-PYXI-270420/775

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
cacagoo					
tv-288zd-2mp					
Improper Authentication	02-04-2020	10	CACAGOO Cloud Storage Intelligent Camera TV-288ZD-2MP with firmware 3.4.2.0919 has weak authentication of TELNET access, leading to root privileges without any password required. **CVE ID : CVE-2020-6852**	N/A	H-CAC-TV-2-270420/776
Missing Authorization	02-04-2020	5	The CACAGOO Cloud Storage Intelligent Camera TV-288ZD-2MP with firmware 3.4.2.0919 allows access to the RTSP service without a password. **CVE ID : CVE-2020-9349**	N/A	H-CAC-TV-2-270420/777
dahua					
sd6al					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go down. **CVE ID : CVE-2020-9499**	N/A	H-DAH-SD6A-270420/778
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may	N/A	H-DAH-SD6A-270420/779

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cause the device to go down. **CVE ID : CVE-2020-9500**		
sd5a					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go down. **CVE ID : CVE-2020-9499**	N/A	H-DAH-SD5A-270420/780
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go down. **CVE ID : CVE-2020-9500**	N/A	H-DAH-SD5A-270420/781
sd1a					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go down. **CVE ID : CVE-2020-9499**	N/A	H-DAH-SD1A-270420/782
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the	N/A	H-DAH-SD1A-270420/783

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go down. **CVE ID : CVE-2020-9500**		
ptz1a					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go down. **CVE ID : CVE-2020-9499**	N/A	H-DAH-PTZ1-270420/784
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go down. **CVE ID : CVE-2020-9500**	N/A	H-DAH-PTZ1-270420/785
sd50					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go down.	N/A	H-DAH-SD50-270420/786

CVSS Scoring Scale	0-1	1-2	2-3	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-2020-9499		
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go down. **CVE ID : CVE-2020-9500**	N/A	H-DAH-SD50-270420/787
sd52c					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go down. **CVE ID : CVE-2020-9499**	N/A	H-DAH-SD52-270420/788
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go down. **CVE ID : CVE-2020-9500**	N/A	H-DAH-SD52-270420/789
ipc-hx5842h					
Buffer Copy without Checking Size of Input ('Classic Buffer	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker	N/A	H-DAH-IPC--270420/790

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			sends a specific DDNS test command, which may cause the device to go down. **CVE ID : CVE-2020-9499**		
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go down. **CVE ID : CVE-2020-9500**	N/A	H-DAH-IPC--270420/791
ipc-hx7842h					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go down. **CVE ID : CVE-2020-9499**	N/A	H-DAH-IPC--270420/792
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go down. **CVE ID : CVE-2020-9500**	N/A	H-DAH-IPC--270420/793
ipc-hx2xxx					
Buffer Copy	09-04-2020	7.5	Some Dahua products	N/A	H-DAH-IPC--

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go down. **CVE ID : CVE-2020-9499**		270420/794
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go down. **CVE ID : CVE-2020-9500**	N/A	H-DAH-IPC--270420/795
ipc-hxxx5x4x					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go down. **CVE ID : CVE-2020-9499**	N/A	H-DAH-IPC--270420/796
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go down.	N/A	H-DAH-IPC--270420/797

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9500		
n42b1p					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go down. **CVE ID : CVE-2020-9499**	N/A	H-DAH-N42B-270420/798
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go down. **CVE ID : CVE-2020-9500**	N/A	H-DAH-N42B-270420/799
n42b2p					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go down. **CVE ID : CVE-2020-9499**	N/A	H-DAH-N42B-270420/800
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker	N/A	H-DAH-N42B-270420/801

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sends a specific log query command, which may cause the device to go down. **CVE ID : CVE-2020-9500**		
n42b3p					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go down. **CVE ID : CVE-2020-9499**	N/A	H-DAH-N42B-270420/802
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go down. **CVE ID : CVE-2020-9500**	N/A	H-DAH-N42B-270420/803
n52a4p					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go down. **CVE ID : CVE-2020-9499**	N/A	H-DAH-N52A-270420/804
Improper	09-04-2020	5	Some products of Dahua	N/A	H-DAH-N52A-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go down. **CVE ID : CVE-2020-9500**		270420/805
n54a4p					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go down. **CVE ID : CVE-2020-9499**	N/A	H-DAH-N54A-270420/806
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go down. **CVE ID : CVE-2020-9500**	N/A	H-DAH-N54A-270420/807
n52b2p					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go	N/A	H-DAH-N52B-270420/808

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			down. **CVE ID : CVE-2020-9499**		
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go down. **CVE ID : CVE-2020-9500**	N/A	H-DAH-N52B-270420/809
n52b5p					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go down. **CVE ID : CVE-2020-9499**	N/A	H-DAH-N52B-270420/810
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go down. **CVE ID : CVE-2020-9500**	N/A	H-DAH-N52B-270420/811
n52b3p					
Buffer Copy without Checking Size of Input	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the	N/A	H-DAH-N52B-270420/812

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			legal account, the attacker sends a specific DDNS test command, which may cause the device to go down. **CVE ID : CVE-2020-9499**		
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go down. **CVE ID : CVE-2020-9500**	N/A	H-DAH-N52B-270420/813
n54b2p					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	09-04-2020	7.5	Some Dahua products have buffer overflow vulnerabilities. After the successful login of the legal account, the attacker sends a specific DDNS test command, which may cause the device to go down. **CVE ID : CVE-2020-9499**	N/A	H-DAH-N54B-270420/814
Improper Input Validation	09-04-2020	5	Some products of Dahua have Denial of Service vulnerabilities. After the successful login of the legal account, the attacker sends a specific log query command, which may cause the device to go down. **CVE ID : CVE-2020-9500**	N/A	H-DAH-N54B-270420/815
Dell					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
latitude_7202					
Use After Free	04-04-2020	7.2	Dell Latitude 7202 Rugged Tablet BIOS versions prior to A28 contain a UAF vulnerability in EFI_BOOT_SERVICES in system management mode. A local unauthenticated attacker may exploit this vulnerability by overwriting the EFI_BOOT_SERVICES structure to execute arbitrary code in system management mode. **CVE ID : CVE-2020-5348**	N/A	H-DEL-LATI-270420/816
r1-2210					
Information Exposure	10-04-2020	5	Dell EMC Networking X-Series firmware versions 3.0.1.2 and older, Dell EMC Networking PC5500 firmware versions 4.1.0.22 and older and Dell EMC PowerEdge VRTX Switch Modules firmware versions 2.0.0.77 and older contain an information disclosure vulnerability. A remote unauthenticated attacker could exploit this vulnerability to retrieve sensitive data by sending a specially crafted request to the affected endpoints. **CVE ID : CVE-2020-5330**	N/A	H-DEL-R1-2-270420/817
r1-2401					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	10-04-2020	5	Dell EMC Networking X-Series firmware versions 3.0.1.2 and older, Dell EMC Networking PC5500 firmware versions 4.1.0.22 and older and Dell EMC PowerEdge VRTX Switch Modules firmware versions 2.0.0.77 and older contain an information disclosure vulnerability. A remote unauthenticated attacker could exploit this vulnerability to retrieve sensitive data by sending a specially crafted request to the affected endpoints. **CVE ID : CVE-2020-5330**	N/A	H-DEL-R1-2-270420/818
pc5500					
Information Exposure	10-04-2020	5	Dell EMC Networking X-Series firmware versions 3.0.1.2 and older, Dell EMC Networking PC5500 firmware versions 4.1.0.22 and older and Dell EMC PowerEdge VRTX Switch Modules firmware versions 2.0.0.77 and older contain an information disclosure vulnerability. A remote unauthenticated attacker could exploit this vulnerability to retrieve sensitive data by sending a specially crafted request to the affected endpoints. **CVE ID : CVE-2020-5330**	N/A	H-DEL-PC55-270420/819

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
x1000					
Information Exposure	10-04-2020	5	Dell EMC Networking X-Series firmware versions 3.0.1.2 and older, Dell EMC Networking PC5500 firmware versions 4.1.0.22 and older and Dell EMC PowerEdge VRTX Switch Modules firmware versions 2.0.0.77 and older contain an information disclosure vulnerability. A remote unauthenticated attacker could exploit this vulnerability to retrieve sensitive data by sending a specially crafted request to the affected endpoints. **CVE ID : CVE-2020-5330**	N/A	H-DEL-X100-270420/820
x4012					
Information Exposure	10-04-2020	5	Dell EMC Networking X-Series firmware versions 3.0.1.2 and older, Dell EMC Networking PC5500 firmware versions 4.1.0.22 and older and Dell EMC PowerEdge VRTX Switch Modules firmware versions 2.0.0.77 and older contain an information disclosure vulnerability. A remote unauthenticated attacker could exploit this vulnerability to retrieve sensitive data by sending a specially crafted request to the affected endpoints.	N/A	H-DEL-X401-270420/821

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5330		
Dlink					
dsl-gs225					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	10-04-2020	6.5	D-Link DSL-GS225 J1 AU_1.0.4 devices allow an admin to execute OS commands by placing shell metacharacters after a supported CLI command, as demonstrated by ping -c1 127.0.0.1; cat/etc/passwd. The CLI is reachable by TELNET. **CVE ID : CVE-2020-6765**	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10165	H-DLI-DSL--270420/822
etentech					
psg-6528vm					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-04-2020	3.5	eten PSG-6528VM 1.1 devices allow XSS via System Contact or System Location. **CVE ID : CVE-2020-11714**	N/A	H-ETE-PSG--270420/823
Fortinet					
fortiadc					
Incorrect Authorization	07-04-2020	6.8	An improper authorization vulnerability in FortiADC may allow a remote authenticated user with low privileges to perform certain actions such as rebooting the system. **CVE ID : CVE-2020-9286**	N/A	H-FOR-FORT-270420/824
Grandstream					
gxp1610					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Link Resolution Before File Access ('Link Following')	14-04-2020	9	Grandstream GXP1600 series firmware 1.0.4.152 and below is vulnerable to authenticated remote command execution when an attacker uploads a specially crafted tar file to the HTTP /cgi-bin/upload_vpntar interface. **CVE ID : CVE-2020-5738**	N/A	H-GRA-GXP1-270420/825
Improper Control of Generation of Code ('Code Injection')	14-04-2020	9	Grandstream GXP1600 series firmware 1.0.4.152 and below is vulnerable to authenticated remote command execution when an attacker adds an OpenVPN up script to the phone's VPN settings via the "Additional Settings" field in the web interface. When the VPN's connection is established, the user defined script is executed with root privileges. **CVE ID : CVE-2020-5739**	N/A	H-GRA-GXP1-270420/826
gxp1615					
Improper Link Resolution Before File Access ('Link Following')	14-04-2020	9	Grandstream GXP1600 series firmware 1.0.4.152 and below is vulnerable to authenticated remote command execution when an attacker uploads a specially crafted tar file to the HTTP /cgi-bin/upload_vpntar interface. **CVE ID : CVE-2020-5738**	N/A	H-GRA-GXP1-270420/827

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	14-04-2020	9	Grandstream GXP1600 series firmware 1.0.4.152 and below is vulnerable to authenticated remote command execution when an attacker adds an OpenVPN up script to the phone's VPN settings via the "Additional Settings" field in the web interface. When the VPN's connection is established, the user defined script is executed with root privileges. **CVE ID : CVE-2020-5739**	N/A	H-GRA-GXP1-270420/828
gxp1620					
Improper Link Resolution Before File Access ('Link Following')	14-04-2020	9	Grandstream GXP1600 series firmware 1.0.4.152 and below is vulnerable to authenticated remote command execution when an attacker uploads a specially crafted tar file to the HTTP /cgi-bin/upload_vpntar interface. **CVE ID : CVE-2020-5738**	N/A	H-GRA-GXP1-270420/829
Improper Control of Generation of Code ('Code Injection')	14-04-2020	9	Grandstream GXP1600 series firmware 1.0.4.152 and below is vulnerable to authenticated remote command execution when an attacker adds an OpenVPN up script to the phone's VPN settings via the "Additional Settings" field in the web interface. When the VPN's connection is established,	N/A	H-GRA-GXP1-270420/830

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the user defined script is executed with root privileges. **CVE ID : CVE-2020-5739**		
gxp1625					
Improper Link Resolution Before File Access ('Link Following')	14-04-2020	9	Grandstream GXP1600 series firmware 1.0.4.152 and below is vulnerable to authenticated remote command execution when an attacker uploads a specially crafted tar file to the HTTP /cgi-bin/upload_vpntar interface. **CVE ID : CVE-2020-5738**	N/A	H-GRA-GXP1-270420/831
Improper Control of Generation of Code ('Code Injection')	14-04-2020	9	Grandstream GXP1600 series firmware 1.0.4.152 and below is vulnerable to authenticated remote command execution when an attacker adds an OpenVPN up script to the phone's VPN settings via the "Additional Settings" field in the web interface. When the VPN's connection is established, the user defined script is executed with root privileges. **CVE ID : CVE-2020-5739**	N/A	H-GRA-GXP1-270420/832
gxp1628					
Improper Link Resolution Before File Access ('Link Following')	14-04-2020	9	Grandstream GXP1600 series firmware 1.0.4.152 and below is vulnerable to authenticated remote command execution when an attacker uploads a	N/A	H-GRA-GXP1-270420/833

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specially crafted tar file to the HTTP /cgi-bin/upload_vpntar interface. **CVE ID : CVE-2020-5738**		
Improper Control of Generation of Code ('Code Injection')	14-04-2020	9	Grandstream GXP1600 series firmware 1.0.4.152 and below is vulnerable to authenticated remote command execution when an attacker adds an OpenVPN up script to the phone's VPN settings via the "Additional Settings" field in the web interface. When the VPN's connection is established, the user defined script is executed with root privileges. **CVE ID : CVE-2020-5739**	N/A	H-GRA-GXP1-270420/834
gxp1630					
Improper Link Resolution Before File Access ('Link Following')	14-04-2020	9	Grandstream GXP1600 series firmware 1.0.4.152 and below is vulnerable to authenticated remote command execution when an attacker uploads a specially crafted tar file to the HTTP /cgi-bin/upload_vpntar interface. **CVE ID : CVE-2020-5738**	N/A	H-GRA-GXP1-270420/835
Improper Control of Generation of Code ('Code Injection')	14-04-2020	9	Grandstream GXP1600 series firmware 1.0.4.152 and below is vulnerable to authenticated remote command execution when an attacker adds an	N/A	H-GRA-GXP1-270420/836

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			OpenVPN up script to the phone's VPN settings via the "Additional Settings" field in the web interface. When the VPN's connection is established, the user defined script is executed with root privileges. **CVE ID : CVE-2020-5739**		
hirschmann					
embedded_ethernet_switch					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-04-2020	7.5	A buffer overflow vulnerability was found in some devices of Hirschmann Automation and Control HiOS and HiSecOS. The vulnerability is due to improper parsing of URL arguments. An attacker could exploit this vulnerability by specially crafting HTTP requests to overflow an internal buffer. The following devices using HiOS Version 07.0.02 and lower are affected: RSP, RSPE, RSPS, RSPL, MSP, EES, EES, EESX, GRS, OS, RED. The following devices using HiSecOS Version 03.2.00 and lower are affected: EAGLE20/30. **CVE ID : CVE-2020-6994**	N/A	H-HIR-EMBE-270420/837
embedded_ethernet_switch_extended					
Buffer Copy without	03-04-2020	7.5	A buffer overflow vulnerability was found in	N/A	H-HIR-EMBE-270420/838

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			some devices of Hirschmann Automation and Control HiOS and HiSecOS. The vulnerability is due to improper parsing of URL arguments. An attacker could exploit this vulnerability by specially crafting HTTP requests to overflow an internal buffer. The following devices using HiOS Version 07.0.02 and lower are affected: RSP, RSPE, RSPS, RSPL, MSP, EES, EES, EESX, GRS, OS, RED. The following devices using HiSecOS Version 03.2.00 and lower are affected: EAGLE20/30. **CVE ID : CVE-2020-6994**		
greyhound_swtich					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-04-2020	7.5	A buffer overflow vulnerability was found in some devices of Hirschmann Automation and Control HiOS and HiSecOS. The vulnerability is due to improper parsing of URL arguments. An attacker could exploit this vulnerability by specially crafting HTTP requests to overflow an internal buffer. The following devices using HiOS Version 07.0.02 and lower are affected: RSP, RSPE,	N/A	H-HIR-GREY-270420/839

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			RSPS, RSPL, MSP, EES, EES, EESX, GRS, OS, RED. The following devices using HiSecOS Version 03.2.00 and lower are affected: EAGLE20/30. **CVE ID : CVE-2020-6994**		
mice_switch_power					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-04-2020	7.5	A buffer overflow vulnerability was found in some devices of Hirschmann Automation and Control HiOS and HiSecOS. The vulnerability is due to improper parsing of URL arguments. An attacker could exploit this vulnerability by specially crafting HTTP requests to overflow an internal buffer. The following devices using HiOS Version 07.0.02 and lower are affected: RSP, RSPE, RSPS, RSPL, MSP, EES, EES, EESX, GRS, OS, RED. The following devices using HiSecOS Version 03.2.00 and lower are affected: EAGLE20/30. **CVE ID : CVE-2020-6994**	N/A	H-HIR-MICE-270420/840
octopus					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-04-2020	7.5	A buffer overflow vulnerability was found in some devices of Hirschmann Automation and Control HiOS and HiSecOS. The	N/A	H-HIR-OCTO-270420/841

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to improper parsing of URL arguments. An attacker could exploit this vulnerability by specially crafting HTTP requests to overflow an internal buffer. The following devices using HiOS Version 07.0.02 and lower are affected: RSP, RSPE, RSPS, RSPL, MSP, EES, EES, EESX, GRS, OS, RED. The following devices using HiSecOS Version 03.2.00 and lower are affected: EAGLE20/30. **CVE ID : CVE-2020-6994**		
prp_redbox					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-04-2020	7.5	A buffer overflow vulnerability was found in some devices of Hirschmann Automation and Control HiOS and HiSecOS. The vulnerability is due to improper parsing of URL arguments. An attacker could exploit this vulnerability by specially crafting HTTP requests to overflow an internal buffer. The following devices using HiOS Version 07.0.02 and lower are affected: RSP, RSPE, RSPS, RSPL, MSP, EES, EES, EESX, GRS, OS, RED. The following devices using HiSecOS Version	N/A	H-HIR-PRP_-270420/842

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			03.2.00 and lower are affected: EAGLE20/30. **CVE ID : CVE-2020-6994**		
rail_switch_power					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-04-2020	7.5	A buffer overflow vulnerability was found in some devices of Hirschmann Automation and Control HiOS and HiSecOS. The vulnerability is due to improper parsing of URL arguments. An attacker could exploit this vulnerability by specially crafting HTTP requests to overflow an internal buffer. The following devices using HiOS Version 07.0.02 and lower are affected: RSP, RSPE, RSPS, RSPL, MSP, EES, EES, EESX, GRS, OS, RED. The following devices using HiSecOS Version 03.2.00 and lower are affected: EAGLE20/30. **CVE ID : CVE-2020-6994**	N/A	H-HIR-RAIL-270420/843
rail_switch_power_enhanced					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-04-2020	7.5	A buffer overflow vulnerability was found in some devices of Hirschmann Automation and Control HiOS and HiSecOS. The vulnerability is due to improper parsing of URL arguments. An attacker could exploit this	N/A	H-HIR-RAIL-270420/844

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by specially crafting HTTP requests to overflow an internal buffer. The following devices using HiOS Version 07.0.02 and lower are affected: RSP, RSPE, RSPS, RSPL, MSP, EES, EES, EESX, GRS, OS, RED. The following devices using HiSecOS Version 03.2.00 and lower are affected: EAGLE20/30. **CVE ID : CVE-2020-6994**		
rail_switch_power_lite					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-04-2020	7.5	A buffer overflow vulnerability was found in some devices of Hirschmann Automation and Control HiOS and HiSecOS. The vulnerability is due to improper parsing of URL arguments. An attacker could exploit this vulnerability by specially crafting HTTP requests to overflow an internal buffer. The following devices using HiOS Version 07.0.02 and lower are affected: RSP, RSPE, RSPS, RSPL, MSP, EES, EES, EESX, GRS, OS, RED. The following devices using HiSecOS Version 03.2.00 and lower are affected: EAGLE20/30. **CVE ID : CVE-2020-6994**	N/A	H-HIR-RAIL-270420/845

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
rail_switch_power_smart					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-04-2020	7.5	A buffer overflow vulnerability was found in some devices of Hirschmann Automation and Control HiOS and HiSecOS. The vulnerability is due to improper parsing of URL arguments. An attacker could exploit this vulnerability by specially crafting HTTP requests to overflow an internal buffer. The following devices using HiOS Version 07.0.02 and lower are affected: RSP, RSPE, RSPS, RSPL, MSP, EES, EES, EESX, GRS, OS, RED. The following devices using HiSecOS Version 03.2.00 and lower are affected: EAGLE20/30. **CVE ID : CVE-2020-6994**	N/A	H-HIR-RAIL-270420/846
eagle20					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-04-2020	7.5	A buffer overflow vulnerability was found in some devices of Hirschmann Automation and Control HiOS and HiSecOS. The vulnerability is due to improper parsing of URL arguments. An attacker could exploit this vulnerability by specially crafting HTTP requests to overflow an internal buffer. The following	N/A	H-HIR-EAGL-270420/847

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			devices using HiOS Version 07.0.02 and lower are affected: RSP, RSPE, RSPS, RSPL, MSP, EES, EES, EESX, GRS, OS, RED. The following devices using HiSecOS Version 03.2.00 and lower are affected: EAGLE20/30. **CVE ID : CVE-2020-6994**		
eagle30					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-04-2020	7.5	A buffer overflow vulnerability was found in some devices of Hirschmann Automation and Control HiOS and HiSecOS. The vulnerability is due to improper parsing of URL arguments. An attacker could exploit this vulnerability by specially crafting HTTP requests to overflow an internal buffer. The following devices using HiOS Version 07.0.02 and lower are affected: RSP, RSPE, RSPS, RSPL, MSP, EES, EES, EESX, GRS, OS, RED. The following devices using HiSecOS Version 03.2.00 and lower are affected: EAGLE20/30. **CVE ID : CVE-2020-6994**	N/A	H-HIR-EAGL-270420/848
hms-networks					
ewon_flexy					
Improper Neutralization	08-04-2020	4.3	A non-persistent XSS (cross-site scripting)	N/A	H-HMS-EWON-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input During Web Page Generation ('Cross-site Scripting')			vulnerability exists in eWON Flexy and Cosy (all firmware versions prior to 14.1s0). An attacker could send a specially crafted URL to initiate a password change for the device. The target must introduce the credentials to the gateway before the attack can be successful. **CVE ID : CVE-2020-10633**		270420/849
ewon_cosy					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-04-2020	4.3	A non-persistent XSS (cross-site scripting) vulnerability exists in eWON Flexy and Cosy (all firmware versions prior to 14.1s0). An attacker could send a specially crafted URL to initiate a password change for the device. The target must introduce the credentials to the gateway before the attack can be successful. **CVE ID : CVE-2020-10633**	N/A	H-HMS-EWON-270420/850
Huawei					
mate_30_pro					
Information Exposure	10-04-2020	4.3	There is an improper authentication vulnerability in several smartphones. Certain function interface in the system does not sufficiently validate the caller's identity in certain	N/A	H-HUA-MATE-270420/851

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			share scenario, successful exploit could cause information disclosure. Affected product versions include:Mate 30 Pro versions Versions earlier than 10.0.0.205(C00E202R7P2);Mate 30 versions Versions earlier than 10.0.0.205(C00E201R7P2). **CVE ID : CVE-2020-1801**		
smartax_ma5600t					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-04-2020	5.2	There is a buffer overflow vulnerability in some Huawei products. The vulnerability can be exploited by an attacker to perform remote code execution on the affected products when the affected product functions as an optical line terminal (OLT). Affected product versions include:SmartAX MA5600T versions V800R013C10, V800R015C00, V800R015C10, V800R017C00, V800R017C10, V800R018C00, V800R018C10; SmartAX MA5800 versions V100R017C00, V100R017C10, V100R018C00, V100R018C10, V100R019C10; SmartAX	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200401-01-overflow-en	H-HUA-SMAR-270420/852

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EA5800 versions V100R018C00, V100R018C10, V100R019C10. **CVE ID : CVE-2020-9067**		
smartax_ma5800					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-04-2020	5.2	There is a buffer overflow vulnerability in some Huawei products. The vulnerability can be exploited by an attacker to perform remote code execution on the affected products when the affected product functions as an optical line terminal (OLT). Affected product versions include:SmartAX MA5600T versions V800R013C10, V800R015C00, V800R015C10, V800R017C00, V800R017C10, V800R018C00, V800R018C10; SmartAX MA5800 versions V100R017C00, V100R017C10, V100R018C00, V100R018C10, V100R019C10; SmartAX EA5800 versions V100R018C00, V100R018C10, V100R019C10. **CVE ID : CVE-2020-9067**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200401-01-overflow-en	H-HUA-SMAR-270420/853
smartax_ea5800					
Buffer Copy	02-04-2020	5.2	There is a buffer overflow	https://ww	H-HUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			vulnerability in some Huawei products. The vulnerability can be exploited by an attacker to perform remote code execution on the affected products when the affected product functions as an optical line terminal (OLT). Affected product versions include:SmartAX MA5600T versions V800R013C10, V800R015C00, V800R015C10, V800R017C00, V800R017C10, V800R018C00, V800R018C10; SmartAX MA5800 versions V100R017C00, V100R017C10, V100R018C00, V100R018C10, V100R019C10; SmartAX EA5800 versions V100R018C00, V100R018C10, V100R019C10. **CVE ID : CVE-2020-9067**	w.huawei.com/en/psirt/security-advisories/huawei-sa-20200401-01-overflow-en	SMAR-270420/854
osca-550					
Improper Validation of Integrity Check Value	10-04-2020	2.1	There is an insufficient integrity validation vulnerability in several products. The device does not sufficiently validate the integrity of certain file in certain loading processes, successful exploit could allow the	N/A	H-HUA-OSCA-270420/855

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to load a crafted file to the device through USB.Affected product versions include:OSCA-550 versions 1.0.1.23(SP2);OSCA-550A versions 1.0.1.23(SP2);OSCA-550AX versions 1.0.1.23(SP2);OSCA-550X versions 1.0.1.23(SP2). **CVE ID : CVE-2020-1802**		
osca-550a					
Improper Validation of Integrity Check Value	10-04-2020	2.1	There is an insufficient integrity validation vulnerability in several products. The device does not sufficiently validate the integrity of certain file in certain loading processes, successful exploit could allow the attacker to load a crafted file to the device through USB.Affected product versions include:OSCA-550 versions 1.0.1.23(SP2);OSCA-550A versions 1.0.1.23(SP2);OSCA-550AX versions 1.0.1.23(SP2);OSCA-550X versions 1.0.1.23(SP2). **CVE ID : CVE-2020-1802**	N/A	H-HUA-OSCA-270420/856
osca-550ax					
Improper Validation of Integrity Check Value	10-04-2020	2.1	There is an insufficient integrity validation vulnerability in several products. The device does	N/A	H-HUA-OSCA-270420/857

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			not sufficiently validate the integrity of certain file in certain loading processes, successful exploit could allow the attacker to load a crafted file to the device through USB.Affected product versions include:OSCA-550 versions 1.0.1.23(SP2);OSCA-550A versions 1.0.1.23(SP2);OSCA-550AX versions 1.0.1.23(SP2);OSCA-550X versions 1.0.1.23(SP2). **CVE ID : CVE-2020-1802**		
osca-550x					
Improper Validation of Integrity Check Value	10-04-2020	2.1	There is an insufficient integrity validation vulnerability in several products. The device does not sufficiently validate the integrity of certain file in certain loading processes, successful exploit could allow the attacker to load a crafted file to the device through USB.Affected product versions include:OSCA-550 versions 1.0.1.23(SP2);OSCA-550A versions 1.0.1.23(SP2);OSCA-550AX versions 1.0.1.23(SP2);OSCA-550X versions 1.0.1.23(SP2). **CVE ID : CVE-2020-1802**	N/A	H-HUA-OSCA-270420/858

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mate_30					
Information Exposure	10-04-2020	4.3	There is an improper authentication vulnerability in several smartphones. Certain function interface in the system does not sufficiently validate the caller's identity in certain share scenario, successful exploit could cause information disclosure. Affected product versions include:Mate 30 Pro versions Versions earlier than 10.0.0.205(C00E202R7P2);Mate 30 versions Versions earlier than 10.0.0.205(C00E201R7P2). **CVE ID : CVE-2020-1801**	N/A	H-HUA-MATE-270420/859
ixsystems					
freenas					
Improper Authentication	08-04-2020	5	An issue was discovered in iXsystems FreeNAS (and TrueNAS) 11.2 before 11.2-u8 and 11.3 before 11.3-U1. It allows a denial of service. The login authentication component has no limits on the length of an authentication message or the rate at which such messages are sent. **CVE ID : CVE-2020-11650**	https://security.ixsystems.com/cves/2020-04-08-cve-2020-11650/	H-IXS-FREE-270420/860
truenas					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	08-04-2020	5	An issue was discovered in iXsystems FreeNAS (and TrueNAS) 11.2 before 11.2-u8 and 11.3 before 11.3-U1. It allows a denial of service. The login authentication component has no limits on the length of an authentication message or the rate at which such messages are sent. **CVE ID : CVE-2020-11650**	https://security.ixsystems.com/cves/2020-04-08-cve-2020-11650/	H-IXS-TRUE-270420/861
Juniper					
srx100					
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session	https://kb.juniper.net/JSA10996	H-JUN-SRX1-270420/862

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
mx2020					
Improper Input	09-04-2020	3.3	Due to a new NDP proxy feature for EVPN leaf	https://kb.juniper.net/J	H-JUN-MX20-270420/863

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			nodes introduced in Junos OS 17.4, crafted NDPv6 packets could transit a Junos device configured as a Broadband Network Gateway (BNG) and reach the EVPN leaf node, causing a stale MAC address entry. This could cause legitimate traffic to be discarded, leading to a Denial of Service (DoS) condition. This issue only affects Junos OS 17.4 and later releases. Prior releases do not support this feature and are unaffected by this vulnerability. This issue only affects IPv6. IPv4 ARP proxy is unaffected by this vulnerability. This issue affects Juniper Networks Junos OS: 17.4 versions prior to 17.4R2-S9, 17.4R3 on MX Series; 18.1 versions prior to 18.1R3-S9 on MX Series; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D33, 18.2X75-D411, 18.2X75-D420, 18.2X75-D60 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3 on MX Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S2, 18.4R3 on MX Series; 19.1 versions prior	SA11012	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to 19.1R1-S4, 19.1R2 on MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series. **CVE ID : CVE-2020-1633**		
Improper Input Validation	08-04-2020	5	The FPC (Flexible PIC Concentrator) of Juniper Networks Junos OS and Junos OS Evolved may restart after processing a specific IPv4 packet. Only packets destined to the device itself, successfully reaching the RE through existing edge and control plane filtering, will be able to cause the FPC restart. When this issue occurs, all traffic via the FPC will be dropped. By continuously sending this specific IPv4 packet, an attacker can repeatedly crash the FPC, causing an extended Denial of Service (DoS) condition. This issue can only occur when processing a specific IPv4 packet. IPv6 packets cannot trigger this issue. This issue affects: Juniper Networks Junos OS on MX Series with MPC10E or MPC11E and PTX10001: 19.2 versions prior to 19.2R1-S4, 19.2R2; 19.3 versions prior to 19.3R2-S2, 19.3R3; 19.4 versions prior to 19.4R1-S1, 19.4R2. Juniper Networks	https://kb.juniper.net/JSA11019	H-JUN-MX20-270420/864

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Junos OS Evolved on on QFX5220, and PTX10003 series: 19.2-EVO versions; 19.3-EVO versions; 19.4-EVO versions prior to 19.4R2-EVO. This issue does not affect Junos OS versions prior to 19.2R1. This issue does not affect Junos OS Evolved versions prior to 19.2R1-EVO. **CVE ID : CVE-2020-1638**		
mx204					
Improper Input Validation	09-04-2020	3.3	Due to a new NDP proxy feature for EVPN leaf nodes introduced in Junos OS 17.4, crafted NDPv6 packets could transit a Junos device configured as a Broadband Network Gateway (BNG) and reach the EVPN leaf node, causing a stale MAC address entry. This could cause legitimate traffic to be discarded, leading to a Denial of Service (DoS) condition. This issue only affects Junos OS 17.4 and later releases. Prior releases do not support this feature and are unaffected by this vulnerability. This issue only affects IPv6. IPv4 ARP proxy is unaffected by this vulnerability. This issue affects Juniper Networks Junos OS: 17.4 versions prior to 17.4R2-	https://kb.juniper.net/JSA11012	H-JUN-MX20-270420/865

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S9, 17.4R3 on MX Series; 18.1 versions prior to 18.1R3-S9 on MX Series; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D33, 18.2X75-D411, 18.2X75-D420, 18.2X75-D60 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3 on MX Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S2, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2 on MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series. **CVE ID : CVE-2020-1633**		
mx240					
Improper Input Validation	09-04-2020	3.3	Due to a new NDP proxy feature for EVPN leaf nodes introduced in Junos OS 17.4, crafted NDPv6 packets could transit a Junos device configured as a Broadband Network Gateway (BNG) and reach the EVPN leaf node, causing a stale MAC address entry. This could cause legitimate traffic to be discarded, leading to a Denial of Service (DoS) condition. This issue only affects Junos OS 17.4 and later releases. Prior releases do not support	https://kb.juniper.net/JSA11012	H-JUN-MX24-270420/866

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			this feature and are unaffected by this vulnerability. This issue only affects IPv6. IPv4 ARP proxy is unaffected by this vulnerability. This issue affects Juniper Networks Junos OS: 17.4 versions prior to 17.4R2-S9, 17.4R3 on MX Series; 18.1 versions prior to 18.1R3-S9 on MX Series; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D33, 18.2X75-D411, 18.2X75-D420, 18.2X75-D60 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3 on MX Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S2, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2 on MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series. **CVE ID : CVE-2020-1633**		
Improper Input Validation	08-04-2020	5	The FPC (Flexible PIC Concentrator) of Juniper Networks Junos OS and Junos OS Evolved may restart after processing a specific IPv4 packet. Only packets destined to the device itself, successfully reaching the RE through existing edge and control plane filtering, will be	https://kb.juniper.net/JSA11019	H-JUN-MX24-270420/867

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			able to cause the FPC restart. When this issue occurs, all traffic via the FPC will be dropped. By continuously sending this specific IPv4 packet, an attacker can repeatedly crash the FPC, causing an extended Denial of Service (DoS) condition. This issue can only occur when processing a specific IPv4 packet. IPv6 packets cannot trigger this issue. This issue affects: Juniper Networks Junos OS on MX Series with MPC10E or MPC11E and PTX10001: 19.2 versions prior to 19.2R1-S4, 19.2R2; 19.3 versions prior to 19.3R2-S2, 19.3R3; 19.4 versions prior to 19.4R1-S1, 19.4R2. Juniper Networks Junos OS Evolved on on QFX5220, and PTX10003 series: 19.2-EVO versions; 19.3-EVO versions; 19.4-EVO versions prior to 19.4R2-EVO. This issue does not affect Junos OS versions prior to 19.2R1. This issue does not affect Junos OS Evolved versions prior to 19.2R1-EVO. **CVE ID : CVE-2020-1638**		
mx40					
Improper Input	09-04-2020	3.3	Due to a new NDP proxy feature for EVPN leaf	https://kb.juniper.net/J	H-JUN-MX40-270420/868

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			nodes introduced in Junos OS 17.4, crafted NDPv6 packets could transit a Junos device configured as a Broadband Network Gateway (BNG) and reach the EVPN leaf node, causing a stale MAC address entry. This could cause legitimate traffic to be discarded, leading to a Denial of Service (DoS) condition. This issue only affects Junos OS 17.4 and later releases. Prior releases do not support this feature and are unaffected by this vulnerability. This issue only affects IPv6. IPv4 ARP proxy is unaffected by this vulnerability. This issue affects Juniper Networks Junos OS: 17.4 versions prior to 17.4R2-S9, 17.4R3 on MX Series; 18.1 versions prior to 18.1R3-S9 on MX Series; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D33, 18.2X75-D411, 18.2X75-D420, 18.2X75-D60 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3 on MX Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S2, 18.4R3 on MX Series; 19.1 versions prior	SA11012	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to 19.1R1-S4, 19.1R2 on MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series. **CVE ID : CVE-2020-1633**		
mx480					
Improper Input Validation	09-04-2020	3.3	Due to a new NDP proxy feature for EVPN leaf nodes introduced in Junos OS 17.4, crafted NDPv6 packets could transit a Junos device configured as a Broadband Network Gateway (BNG) and reach the EVPN leaf node, causing a stale MAC address entry. This could cause legitimate traffic to be discarded, leading to a Denial of Service (DoS) condition. This issue only affects Junos OS 17.4 and later releases. Prior releases do not support this feature and are unaffected by this vulnerability. This issue only affects IPv6. IPv4 ARP proxy is unaffected by this vulnerability. This issue affects Juniper Networks Junos OS: 17.4 versions prior to 17.4R2-S9, 17.4R3 on MX Series; 18.1 versions prior to 18.1R3-S9 on MX Series; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-	https://kb.juniper.net/JSA11012	H-JUN-MX48-270420/869

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			D33, 18.2X75-D411, 18.2X75-D420, 18.2X75-D60 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3 on MX Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S2, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2 on MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series. **CVE ID : CVE-2020-1633**		
Improper Input Validation	08-04-2020	5	The FPC (Flexible PIC Concentrator) of Juniper Networks Junos OS and Junos OS Evolved may restart after processing a specific IPv4 packet. Only packets destined to the device itself, successfully reaching the RE through existing edge and control plane filtering, will be able to cause the FPC restart. When this issue occurs, all traffic via the FPC will be dropped. By continuously sending this specific IPv4 packet, an attacker can repeatedly crash the FPC, causing an extended Denial of Service (DoS) condition. This issue can only occur when processing a specific IPv4 packet. IPv6 packets cannot trigger this issue. This issue affects: Juniper Networks	https://kb.juniper.net/JSA11019	H-JUN-MX48-270420/870

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Junos OS on MX Series with MPC10E or MPC11E and PTX10001: 19.2 versions prior to 19.2R1-S4, 19.2R2; 19.3 versions prior to 19.3R2-S2, 19.3R3; 19.4 versions prior to 19.4R1-S1, 19.4R2. Juniper Networks Junos OS Evolved on on QFX5220, and PTX10003 series: 19.2-EVO versions; 19.3-EVO versions; 19.4-EVO versions prior to 19.4R2-EVO. This issue does not affect Junos OS versions prior to 19.2R1. This issue does not affect Junos OS Evolved versions prior to 19.2R1-EVO. **CVE ID : CVE-2020-1638**		
mx5					
Improper Input Validation	09-04-2020	3.3	Due to a new NDP proxy feature for EVPN leaf nodes introduced in Junos OS 17.4, crafted NDPv6 packets could transit a Junos device configured as a Broadband Network Gateway (BNG) and reach the EVPN leaf node, causing a stale MAC address entry. This could cause legitimate traffic to be discarded, leading to a Denial of Service (DoS) condition. This issue only affects Junos OS 17.4 and later releases. Prior releases do not support	https://kb.juniper.net/JSA11012	H-JUN-MX5-270420/871

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			this feature and are unaffected by this vulnerability. This issue only affects IPv6. IPv4 ARP proxy is unaffected by this vulnerability. This issue affects Juniper Networks Junos OS: 17.4 versions prior to 17.4R2-S9, 17.4R3 on MX Series; 18.1 versions prior to 18.1R3-S9 on MX Series; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D33, 18.2X75-D411, 18.2X75-D420, 18.2X75-D60 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3 on MX Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S2, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2 on MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series. **CVE ID : CVE-2020-1633**		
mx80					
Improper Input Validation	09-04-2020	3.3	Due to a new NDP proxy feature for EVPN leaf nodes introduced in Junos OS 17.4, crafted NDPv6 packets could transit a Junos device configured as a Broadband Network Gateway (BNG) and reach the EVPN leaf node,	https://kb.juniper.net/JSA11012	H-JUN-MX80-270420/872

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			causing a stale MAC address entry. This could cause legitimate traffic to be discarded, leading to a Denial of Service (DoS) condition. This issue only affects Junos OS 17.4 and later releases. Prior releases do not support this feature and are unaffected by this vulnerability. This issue only affects IPv6. IPv4 ARP proxy is unaffected by this vulnerability. This issue affects Juniper Networks Junos OS: 17.4 versions prior to 17.4R2-S9, 17.4R3 on MX Series; 18.1 versions prior to 18.1R3-S9 on MX Series; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D33, 18.2X75-D411, 18.2X75-D420, 18.2X75-D60 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3 on MX Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S2, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2 on MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series. **CVE ID : CVE-2020-1633**		
mx960					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	09-04-2020	3.3	Due to a new NDP proxy feature for EVPN leaf nodes introduced in Junos OS 17.4, crafted NDPv6 packets could transit a Junos device configured as a Broadband Network Gateway (BNG) and reach the EVPN leaf node, causing a stale MAC address entry. This could cause legitimate traffic to be discarded, leading to a Denial of Service (DoS) condition. This issue only affects Junos OS 17.4 and later releases. Prior releases do not support this feature and are unaffected by this vulnerability. This issue only affects IPv6. IPv4 ARP proxy is unaffected by this vulnerability. This issue affects Juniper Networks Junos OS: 17.4 versions prior to 17.4R2-S9, 17.4R3 on MX Series; 18.1 versions prior to 18.1R3-S9 on MX Series; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D33, 18.2X75-D411, 18.2X75-D420, 18.2X75-D60 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3 on MX Series; 18.4 versions prior to 18.4R1-S5,	https://kb.juniper.net/JSA11012	H-JUN-MX96-270420/873

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.4R2-S2, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2 on MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series. **CVE ID : CVE-2020-1633**		
Improper Input Validation	08-04-2020	5	The FPC (Flexible PIC Concentrator) of Juniper Networks Junos OS and Junos OS Evolved may restart after processing a specific IPv4 packet. Only packets destined to the device itself, successfully reaching the RE through existing edge and control plane filtering, will be able to cause the FPC restart. When this issue occurs, all traffic via the FPC will be dropped. By continuously sending this specific IPv4 packet, an attacker can repeatedly crash the FPC, causing an extended Denial of Service (DoS) condition. This issue can only occur when processing a specific IPv4 packet. IPv6 packets cannot trigger this issue. This issue affects: Juniper Networks Junos OS on MX Series with MPC10E or MPC11E and PTX10001: 19.2 versions prior to 19.2R1-S4, 19.2R2; 19.3 versions prior to 19.3R2-S2, 19.3R3; 19.4 versions	https://kb.juniper.net/JSA11019	H-JUN-MX96-270420/874

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.4R1-S1, 19.4R2. Juniper Networks Junos OS Evolved on on QFX5220, and PTX10003 series: 19.2-EVO versions; 19.3-EVO versions; 19.4-EVO versions prior to 19.4R2-EVO. This issue does not affect Junos OS versions prior to 19.2R1. This issue does not affect Junos OS Evolved versions prior to 19.2R1-EVO. **CVE ID : CVE-2020-1638**		
ptx1000					
Improper Initialization	08-04-2020	7.8	This issue occurs on Juniper Networks Junos OS devices which do not support Advanced Forwarding Interface (AFI) / Advanced Forwarding Toolkit (AFT). Devices using AFI and AFT are not exploitable to this issue. An improper initialization of memory in the packet forwarding architecture in Juniper Networks Junos OS non-AFI/AFT platforms which may lead to a Denial of Service (DoS) vulnerability being exploited when a genuine packet is received and inspected by non-AFT/AFI sFlow and when the device is also configured with firewall policers. This first	N/A	H-JUN-PTX1-270420/875

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			genuine packet received and inspected by sampled flow (sFlow) through a specific firewall policer will cause the device to reboot. After the reboot has completed, if the device receives and sFlow inspects another genuine packet seen through a specific firewall policer, the device will generate a core file and reboot. Continued inspection of these genuine packets will create an extended Denial of Service (DoS) condition. Depending on the method for service restoration, e.g. hard boot or soft reboot, a core file may or may not be generated the next time the packet is received and inspected by sFlow. This issue affects: Juniper Networks Junos OS 17.4 versions prior to 17.4R2-S9, 17.4R3 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.1 versions prior to 18.1R3-S9 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.2X75 versions prior to 18.2X75-D12, 18.2X75-D30 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.2 versions prior to 18.2R3		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on PTX1000 and PTX10000 Series, QFX10000 Series; 18.3 versions prior to 18.3R3 on PTX1000 and PTX10000 Series, QFX10000 Series. This issue is not applicable to Junos OS versions before 17.4R1. This issue is not applicable to Junos OS Evolved or Junos OS with Advanced Forwarding Toolkit (AFT) forwarding implementations which use a different implementation of sFlow. The following example information is unrelated to this issue and is provided solely to assist you with determining if you have AFT or not. Example: A Junos OS device which supports the use of EVPN signaled VPWS with Flexible Cross Connect uses the AFT implementation. Since this configuration requires support and use of the AFT implementation to support this configuration, the device is not vulnerable to this issue as the sFlow implementation is different using the AFT architecture. For further details about AFT visit the		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AFI / AFT are in the links below. If you are uncertain if you use the AFI/AFT implementation or not, there are configuration examples in the links below which you may use to determine if you are vulnerable to this issue or not. If the commands work, you are. If not, you are not. You may also use the Feature Explorer to determine if AFI/AFT is supported or not. If you are still uncertain, please contact your support resources. **CVE ID : CVE-2020-1617**		
ptx10002					
Improper Initialization	08-04-2020	7.8	This issue occurs on Juniper Networks Junos OS devices which do not support Advanced Forwarding Interface (AFI) / Advanced Forwarding Toolkit (AFT). Devices using AFI and AFT are not exploitable to this issue. An improper initialization of memory in the packet forwarding architecture in Juniper Networks Junos OS non-AFI/AFT platforms which may lead to a Denial of Service (DoS) vulnerability being exploited when a genuine packet is received and	N/A	H-JUN-PTX1-270420/876

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			inspected by non-AFT/AFI sFlow and when the device is also configured with firewall policers. This first genuine packet received and inspected by sampled flow (sFlow) through a specific firewall policer will cause the device to reboot. After the reboot has completed, if the device receives and sFlow inspects another genuine packet seen through a specific firewall policer, the device will generate a core file and reboot. Continued inspection of these genuine packets will create an extended Denial of Service (DoS) condition. Depending on the method for service restoration, e.g. hard boot or soft reboot, a core file may or may not be generated the next time the packet is received and inspected by sFlow. This issue affects: Juniper Networks Junos OS 17.4 versions prior to 17.4R2-S9, 17.4R3 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.1 versions prior to 18.1R3-S9 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.2X75 versions prior to		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.2X75-D12, 18.2X75-D30 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.2 versions prior to 18.2R3 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.3 versions prior to 18.3R3 on PTX1000 and PTX10000 Series, QFX10000 Series. This issue is not applicable to Junos OS versions before 17.4R1. This issue is not applicable to Junos OS Evolved or Junos OS with Advanced Forwarding Toolkit (AFT) forwarding implementations which use a different implementation of sFlow. The following example information is unrelated to this issue and is provided solely to assist you with determining if you have AFT or not. Example: A Junos OS device which supports the use of EVPN signaled VPWS with Flexible Cross Connect uses the AFT implementation. Since this configuration requires support and use of the AFT implementation to support this configuration, the device is not vulnerable to this		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue as the sFlow implementation is different using the AFT architecture. For further details about AFT visit the AFI / AFT are in the links below. If you are uncertain if you use the AFI/AFT implementation or not, there are configuration examples in the links below which you may use to determine if you are vulnerable to this issue or not. If the commands work, you are. If not, you are not. You may also use the Feature Explorer to determine if AFI/AFT is supported or not. If you are still uncertain, please contact your support resources. **CVE ID : CVE-2020-1617**		
ptx10008					
Improper Initialization	08-04-2020	7.8	This issue occurs on Juniper Networks Junos OS devices which do not support Advanced Forwarding Interface (AFI) / Advanced Forwarding Toolkit (AFT). Devices using AFI and AFT are not exploitable to this issue. An improper initialization of memory in the packet forwarding architecture in Juniper Networks Junos OS non-AFI/AFT	N/A	H-JUN-PTX1-270420/877

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			platforms which may lead to a Denial of Service (DoS) vulnerability being exploited when a genuine packet is received and inspected by non-AFT/AFI sFlow and when the device is also configured with firewall policers. This first genuine packet received and inspected by sampled flow (sFlow) through a specific firewall policer will cause the device to reboot. After the reboot has completed, if the device receives and sFlow inspects another genuine packet seen through a specific firewall policer, the device will generate a core file and reboot. Continued inspection of these genuine packets will create an extended Denial of Service (DoS) condition. Depending on the method for service restoration, e.g. hard boot or soft reboot, a core file may or may not be generated the next time the packet is received and inspected by sFlow. This issue affects: Juniper Networks Junos OS 17.4 versions prior to 17.4R2-S9, 17.4R3 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.1		

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 18.1R3-S9 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.2X75 versions prior to 18.2X75-D12, 18.2X75-D30 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.2 versions prior to 18.2R3 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.3 versions prior to 18.3R3 on PTX1000 and PTX10000 Series, QFX10000 Series. This issue is not applicable to Junos OS versions before 17.4R1. This issue is not applicable to Junos OS Evolved or Junos OS with Advanced Forwarding Toolkit (AFT) forwarding implementations which use a different implementation of sFlow. The following example information is unrelated to this issue and is provided solely to assist you with determining if you have AFT or not. Example: A Junos OS device which supports the use of EVPN signaled VPWS with Flexible Cross Connect uses the AFT implementation. Since this configuration requires support and use		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of the AFT implementation to support this configuration, the device is not vulnerable to this issue as the sFlow implementation is different using the AFT architecture. For further details about AFT visit the AFI / AFT are in the links below. If you are uncertain if you use the AFI/AFT implementation or not, there are configuration examples in the links below which you may use to determine if you are vulnerable to this issue or not. If the commands work, you are. If not, you are not. You may also use the Feature Explorer to determine if AFI/AFT is supported or not. If you are still uncertain, please contact your support resources. **CVE ID : CVE-2020-1617**		
ptx10016					
Improper Initialization	08-04-2020	7.8	This issue occurs on Juniper Networks Junos OS devices which do not support Advanced Forwarding Interface (AFI) / Advanced Forwarding Toolkit (AFT). Devices using AFI and AFT are not exploitable to this issue.	N/A	H-JUN-PTX1-270420/878

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			An improper initialization of memory in the packet forwarding architecture in Juniper Networks Junos OS non-AFI/AFT platforms which may lead to a Denial of Service (DoS) vulnerability being exploited when a genuine packet is received and inspected by non-AFT/AFI sFlow and when the device is also configured with firewall policers. This first genuine packet received and inspected by sampled flow (sFlow) through a specific firewall policer will cause the device to reboot. After the reboot has completed, if the device receives and sFlow inspects another genuine packet seen through a specific firewall policer, the device will generate a core file and reboot. Continued inspection of these genuine packets will create an extended Denial of Service (DoS) condition. Depending on the method for service restoration, e.g. hard boot or soft reboot, a core file may or may not be generated the next time the packet is received and inspected by sFlow. This issue affects: Juniper		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS 17.4 versions prior to 17.4R2-S9, 17.4R3 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.1 versions prior to 18.1R3-S9 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.2X75 versions prior to 18.2X75-D12, 18.2X75-D30 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.2 versions prior to 18.2R3 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.3 versions prior to 18.3R3 on PTX1000 and PTX10000 Series, QFX10000 Series. This issue is not applicable to Junos OS versions before 17.4R1. This issue is not applicable to Junos OS Evolved or Junos OS with Advanced Forwarding Toolkit (AFT) forwarding implementations which use a different implementation of sFlow. The following example information is unrelated to this issue and is provided solely to assist you with determining if you have AFT or not. Example: A Junos OS device which supports the use of EVPN signaled		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			VPWS with Flexible Cross Connect uses the AFT implementation. Since this configuration requires support and use of the AFT implementation to support this configuration, the device is not vulnerable to this issue as the sFlow implementation is different using the AFT architecture. For further details about AFT visit the AFI / AFT are in the links below. If you are uncertain if you use the AFI/AFT implementation or not, there are configuration examples in the links below which you may use to determine if you are vulnerable to this issue or not. If the commands work, you are. If not, you are not. You may also use the Feature Explorer to determine if AFI/AFT is supported or not. If you are still uncertain, please contact your support resources. **CVE ID : CVE-2020-1617**		
ptx3000					
Improper Initialization	08-04-2020	7.8	This issue occurs on Juniper Networks Junos OS devices which do not support Advanced Forwarding Interface	N/A	H-JUN-PTX3-270420/879

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(AFI) / Advanced Forwarding Toolkit (AFT). Devices using AFI and AFT are not exploitable to this issue. An improper initialization of memory in the packet forwarding architecture in Juniper Networks Junos OS non-AFI/AFT platforms which may lead to a Denial of Service (DoS) vulnerability being exploited when a genuine packet is received and inspected by non-AFT/AFI sFlow and when the device is also configured with firewall policers. This first genuine packet received and inspected by sampled flow (sFlow) through a specific firewall policer will cause the device to reboot. After the reboot has completed, if the device receives and sFlow inspects another genuine packet seen through a specific firewall policer, the device will generate a core file and reboot. Continued inspection of these genuine packets will create an extended Denial of Service (DoS) condition. Depending on the method for service restoration, e.g. hard boot or soft reboot, a core file		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may or may not be generated the next time the packet is received and inspected by sFlow. This issue affects: Juniper Networks Junos OS 17.4 versions prior to 17.4R2-S9, 17.4R3 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.1 versions prior to 18.1R3-S9 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.2X75 versions prior to 18.2X75-D12, 18.2X75-D30 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.2 versions prior to 18.2R3 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.3 versions prior to 18.3R3 on PTX1000 and PTX10000 Series, QFX10000 Series. This issue is not applicable to Junos OS versions before 17.4R1. This issue is not applicable to Junos OS Evolved or Junos OS with Advanced Forwarding Toolkit (AFT) forwarding implementations which use a different implementation of sFlow. The following example information is unrelated to this issue and is provided solely to assist		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			you with determining if you have AFT or not. Example: A Junos OS device which supports the use of EVPN signaled VPWS with Flexible Cross Connect uses the AFT implementation. Since this configuration requires support and use of the AFT implementation to support this configuration, the device is not vulnerable to this issue as the sFlow implementation is different using the AFT architecture. For further details about AFT visit the AFI / AFT are in the links below. If you are uncertain if you use the AFI/AFT implementation or not, there are configuration examples in the links below which you may use to determine if you are vulnerable to this issue or not. If the commands work, you are. If not, you are not. You may also use the Feature Explorer to determine if AFI/AFT is supported or not. If you are still uncertain, please contact your support resources. **CVE ID : CVE-2020-1617**		
ptx5000					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Initialization	08-04-2020	7.8	This issue occurs on Juniper Networks Junos OS devices which do not support Advanced Forwarding Interface (AFI) / Advanced Forwarding Toolkit (AFT). Devices using AFI and AFT are not exploitable to this issue. An improper initialization of memory in the packet forwarding architecture in Juniper Networks Junos OS non-AFI/AFT platforms which may lead to a Denial of Service (DoS) vulnerability being exploited when a genuine packet is received and inspected by non-AFT/AFI sFlow and when the device is also configured with firewall policers. This first genuine packet received and inspected by sampled flow (sFlow) through a specific firewall policer will cause the device to reboot. After the reboot has completed, if the device receives and sFlow inspects another genuine packet seen through a specific firewall policer, the device will generate a core file and reboot. Continued inspection of these genuine packets will create an extended Denial	N/A	H-JUN-PTX5-270420/880

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of Service (DoS) condition. Depending on the method for service restoration, e.g. hard boot or soft reboot, a core file may or may not be generated the next time the packet is received and inspected by sFlow. This issue affects: Juniper Networks Junos OS 17.4 versions prior to 17.4R2-S9, 17.4R3 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.1 versions prior to 18.1R3-S9 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.2X75 versions prior to 18.2X75-D12, 18.2X75-D30 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.2 versions prior to 18.2R3 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.3 versions prior to 18.3R3 on PTX1000 and PTX10000 Series, QFX10000 Series. This issue is not applicable to Junos OS versions before 17.4R1. This issue is not applicable to Junos OS Evolved or Junos OS with Advanced Forwarding Toolkit (AFT) forwarding implementations which use a different		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			implementation of sFlow. The following example information is unrelated to this issue and is provided solely to assist you with determining if you have AFT or not. Example: A Junos OS device which supports the use of EVPN signaled VPWS with Flexible Cross Connect uses the AFT implementation. Since this configuration requires support and use of the AFT implementation to support this configuration, the device is not vulnerable to this issue as the sFlow implementation is different using the AFT architecture. For further details about AFT visit the AFI / AFT are in the links below. If you are uncertain if you use the AFI/AFT implementation or not, there are configuration examples in the links below which you may use to determine if you are vulnerable to this issue or not. If the commands work, you are. If not, you are not. You may also use the Feature Explorer to determine if AFI/AFT is supported or not. If you are still		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			uncertain, please contact your support resources. **CVE ID : CVE-2020-1617**		
qfx3000-g					
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-	https://kb.juniper.net/JSA10996	H-JUN-QFX3-270420/881

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
qfx3000-m					
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent	https://kb.juniper.net/JSA10996	H-JUN-QFX3-270420/882

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
ex9200					
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-	https://kb.juniper.net/JSA10996	H-JUN-EX92-270420/883

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
qfx3008-i					
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an	https://kb.juniper.net/JSA10996	H-JUN-QFX3-270420/884

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110,		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
ex9250					
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48	https://kb.juniper.net/JSA10996	H-JUN-EX92-270420/885

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
qfx3100					
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec	https://kb.juniper.net/JSA10996	H-JUN-QFX3-270420/886

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
qfx3600-i					
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec	https://kb.juniper.net/JSA10996	H-JUN-QFX3-270420/887

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
srx4600					
Improper Input Validation	08-04-2020	4.3	On High-End SRX Series devices, in specific configurations and when specific networking events or operator actions	N/A	H-JUN-SRX4-270420/888

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			occur, an SPC receiving genuine multicast traffic may core. Subsequently, all FPCs in a chassis may reset causing a Denial of Service. This issue affects both IPv4 and IPv6. This issue affects: Juniper Networks Junos OS 12.3X48 version 12.3X48-D80 and later versions prior to 12.3X48-D95 on High-End SRX Series. This issue does not affect Branch SRX Series devices. **CVE ID : CVE-2020-1634**		
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session	https://kb.juniper.net/JSA10996	H-JUN-SRX4-270420/889

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
nfx150					
Improper Input	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation	https://kb.juniper.net/J	H-JUN-NFX1-270420/890

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions	SA10996	

CVSS Scoring Scale	0-1	1-2	2-3	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 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
nfx250					
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the	https://kb.juniper.net/JSA10996	H-JUN-NFX2-270420/891

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	08-04-2020	9.3	A Use of Hard-coded Credentials vulnerability exists in the NFX250 Series for the vSRX Virtual Network Function (VNF) instance, which allows an attacker to take control of the vSRX VNF instance if they have the ability to access an administrative service (e.g. SSH) on the VNF, either locally, or through the network. This issue only affects the NFX250 Series vSRX VNF. No other products or platforms are affected. This issue is only applicable to environments where the vSRX VNF root password has not been configured. This issue affects the Juniper Networks NFX250 Network Services Platform vSRX VNF instance on versions prior to 19.2R1. **CVE ID : CVE-2020-1614**	N/A	H-JUN-NFX2-270420/892
ptx10000					
Improper Initialization	08-04-2020	7.8	This issue occurs on Juniper Networks Junos OS devices which do not support Advanced Forwarding Interface (AFI) / Advanced Forwarding Toolkit (AFT). Devices using AFI and AFT are not exploitable to this issue.	N/A	H-JUN-PTX1-270420/893

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			An improper initialization of memory in the packet forwarding architecture in Juniper Networks Junos OS non-AFI/AFT platforms which may lead to a Denial of Service (DoS) vulnerability being exploited when a genuine packet is received and inspected by non-AFT/AFI sFlow and when the device is also configured with firewall policers. This first genuine packet received and inspected by sampled flow (sFlow) through a specific firewall policer will cause the device to reboot. After the reboot has completed, if the device receives and sFlow inspects another genuine packet seen through a specific firewall policer, the device will generate a core file and reboot. Continued inspection of these genuine packets will create an extended Denial of Service (DoS) condition. Depending on the method for service restoration, e.g. hard boot or soft reboot, a core file may or may not be generated the next time the packet is received and inspected by sFlow. This issue affects: Juniper		

CVSS Scoring Scale	0-1	1-2	2-3	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 17.4 versions prior to 17.4R2-S9, 17.4R3 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.1 versions prior to 18.1R3-S9 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.2X75 versions prior to 18.2X75-D12, 18.2X75-D30 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.2 versions prior to 18.2R3 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.3 versions prior to 18.3R3 on PTX1000 and PTX10000 Series, QFX10000 Series. This issue is not applicable to Junos OS versions before 17.4R1. This issue is not applicable to Junos OS Evolved or Junos OS with Advanced Forwarding Toolkit (AFT) forwarding implementations which use a different implementation of sFlow. The following example information is unrelated to this issue and is provided solely to assist you with determining if you have AFT or not. Example: A Junos OS device which supports the use of EVPN signaled		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			VPWS with Flexible Cross Connect uses the AFT implementation. Since this configuration requires support and use of the AFT implementation to support this configuration, the device is not vulnerable to this issue as the sFlow implementation is different using the AFT architecture. For further details about AFT visit the AFI / AFT are in the links below. If you are uncertain if you use the AFI/AFT implementation or not, there are configuration examples in the links below which you may use to determine if you are vulnerable to this issue or not. If the commands work, you are. If not, you are not. You may also use the Feature Explorer to determine if AFI/AFT is supported or not. If you are still uncertain, please contact your support resources. **CVE ID : CVE-2020-1617**		
ptx10001					
Improper Initialization	08-04-2020	7.8	This issue occurs on Juniper Networks Junos OS devices which do not support Advanced Forwarding Interface	N/A	H-JUN-PTX1-270420/894

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(AFI) / Advanced Forwarding Toolkit (AFT). Devices using AFI and AFT are not exploitable to this issue. An improper initialization of memory in the packet forwarding architecture in Juniper Networks Junos OS non-AFI/AFT platforms which may lead to a Denial of Service (DoS) vulnerability being exploited when a genuine packet is received and inspected by non-AFT/AFI sFlow and when the device is also configured with firewall policers. This first genuine packet received and inspected by sampled flow (sFlow) through a specific firewall policer will cause the device to reboot. After the reboot has completed, if the device receives and sFlow inspects another genuine packet seen through a specific firewall policer, the device will generate a core file and reboot. Continued inspection of these genuine packets will create an extended Denial of Service (DoS) condition. Depending on the method for service restoration, e.g. hard boot or soft reboot, a core file		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may or may not be generated the next time the packet is received and inspected by sFlow. This issue affects: Juniper Networks Junos OS 17.4 versions prior to 17.4R2-S9, 17.4R3 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.1 versions prior to 18.1R3-S9 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.2X75 versions prior to 18.2X75-D12, 18.2X75-D30 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.2 versions prior to 18.2R3 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.3 versions prior to 18.3R3 on PTX1000 and PTX10000 Series, QFX10000 Series. This issue is not applicable to Junos OS versions before 17.4R1. This issue is not applicable to Junos OS Evolved or Junos OS with Advanced Forwarding Toolkit (AFT) forwarding implementations which use a different implementation of sFlow. The following example information is unrelated to this issue and is provided solely to assist		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			you with determining if you have AFT or not. Example: A Junos OS device which supports the use of EVPN signaled VPWS with Flexible Cross Connect uses the AFT implementation. Since this configuration requires support and use of the AFT implementation to support this configuration, the device is not vulnerable to this issue as the sFlow implementation is different using the AFT architecture. For further details about AFT visit the AFI / AFT are in the links below. If you are uncertain if you use the AFI/AFT implementation or not, there are configuration examples in the links below which you may use to determine if you are vulnerable to this issue or not. If the commands work, you are. If not, you are not. You may also use the Feature Explorer to determine if AFI/AFT is supported or not. If you are still uncertain, please contact your support resources. **CVE ID : CVE-2020-1617**		
ptx10003					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	08-04-2020	5	The FPC (Flexible PIC Concentrator) of Juniper Networks Junos OS and Junos OS Evolved may restart after processing a specific IPv4 packet. Only packets destined to the device itself, successfully reaching the RE through existing edge and control plane filtering, will be able to cause the FPC restart. When this issue occurs, all traffic via the FPC will be dropped. By continuously sending this specific IPv4 packet, an attacker can repeatedly crash the FPC, causing an extended Denial of Service (DoS) condition. This issue can only occur when processing a specific IPv4 packet. IPv6 packets cannot trigger this issue. This issue affects: Juniper Networks Junos OS on MX Series with MPC10E or MPC11E and PTX10001: 19.2 versions prior to 19.2R1-S4, 19.2R2; 19.3 versions prior to 19.3R2-S2, 19.3R3; 19.4 versions prior to 19.4R1-S1, 19.4R2. Juniper Networks Junos OS Evolved on on QFX5220, and PTX10003 series: 19.2-EVO versions; 19.3-EVO versions; 19.4-EVO versions prior to	https://kb.juniper.net/JSA11019	H-JUN-PTX1-270420/895

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.4R2-EVO. This issue does not affect Junos OS versions prior to 19.2R1. This issue does not affect Junos OS Evolved versions prior to 19.2R1-EVO. **CVE ID : CVE-2020-1638**		
Improper Initialization	08-04-2020	7.8	This issue occurs on Juniper Networks Junos OS devices which do not support Advanced Forwarding Interface (AFI) / Advanced Forwarding Toolkit (AFT). Devices using AFI and AFT are not exploitable to this issue. An improper initialization of memory in the packet forwarding architecture in Juniper Networks Junos OS non-AFI/AFT platforms which may lead to a Denial of Service (DoS) vulnerability being exploited when a genuine packet is received and inspected by non-AFT/AFI sFlow and when the device is also configured with firewall policers. This first genuine packet received and inspected by sampled flow (sFlow) through a specific firewall policer will cause the device to reboot. After the reboot has completed, if the device receives and sFlow inspects another genuine	N/A	H-JUN-PTX1-270420/896

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			packet seen through a specific firewall policer, the device will generate a core file and reboot. Continued inspection of these genuine packets will create an extended Denial of Service (DoS) condition. Depending on the method for service restoration, e.g. hard boot or soft reboot, a core file may or may not be generated the next time the packet is received and inspected by sFlow. This issue affects: Juniper Networks Junos OS 17.4 versions prior to 17.4R2-S9, 17.4R3 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.1 versions prior to 18.1R3-S9 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.2X75 versions prior to 18.2X75-D12, 18.2X75-D30 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.2 versions prior to 18.2R3 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.3 versions prior to 18.3R3 on PTX1000 and PTX10000 Series, QFX10000 Series. This issue is not applicable to Junos OS versions before		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			17.4R1. This issue is not applicable to Junos OS Evolved or Junos OS with Advanced Forwarding Toolkit (AFT) forwarding implementations which use a different implementation of sFlow. The following example information is unrelated to this issue and is provided solely to assist you with determining if you have AFT or not. Example: A Junos OS device which supports the use of EVPN signaled VPWS with Flexible Cross Connect uses the AFT implementation. Since this configuration requires support and use of the AFT implementation to support this configuration, the device is not vulnerable to this issue as the sFlow implementation is different using the AFT architecture. For further details about AFT visit the AFI / AFT are in the links below. If you are uncertain if you use the AFI/AFT implementation or not, there are configuration examples in the links below which you may use to determine if you are vulnerable to this		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue or not. If the commands work, you are. If not, you are not. You may also use the Feature Explorer to determine if AFI/AFT is supported or not. If you are still uncertain, please contact your support resources. **CVE ID : CVE-2020-1617**		
qfx5220					
Improper Authentication	08-04-2020	6.9	On Juniper Networks EX and QFX Series, an authentication bypass vulnerability may allow a user connected to the console port to login as root without any password. This issue might only occur in certain scenarios: • At the first reboot after performing device factory reset using the command "request system zeroize"; or • A temporary moment during the first reboot after the software upgrade when the device configured in Virtual Chassis mode. This issue affects Juniper Networks Junos OS on EX and QFX Series: 14.1X53 versions prior to 14.1X53-D53; 15.1 versions prior to 15.1R7-S4; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S4; 17.1	https://kb.juniper.net/JSA11001	H-JUN-QFX5-270420/897

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 17.1R2-S11, 17.1R3-S1; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S6; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S8; 18.2 versions prior to 18.2R2; 18.3 versions prior to 18.3R1-S7, 18.3R2. This issue does not affect Juniper Networks Junos OS 12.3. **CVE ID : CVE-2020-1618**		
Improper Input Validation	08-04-2020	5	The FPC (Flexible PIC Concentrator) of Juniper Networks Junos OS and Junos OS Evolved may restart after processing a specific IPv4 packet. Only packets destined to the device itself, successfully reaching the RE through existing edge and control plane filtering, will be able to cause the FPC restart. When this issue occurs, all traffic via the FPC will be dropped. By continuously sending this specific IPv4 packet, an attacker can repeatedly crash the FPC, causing an extended Denial of Service (DoS) condition. This issue can only occur when processing a specific IPv4 packet. IPv6 packets cannot trigger this issue. This issue	https://kb.juniper.net/JSA11019	H-JUN-QFX5-270420/898

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affects: Juniper Networks Junos OS on MX Series with MPC10E or MPC11E and PTX10001: 19.2 versions prior to 19.2R1-S4, 19.2R2; 19.3 versions prior to 19.3R2-S2, 19.3R3; 19.4 versions prior to 19.4R1-S1, 19.4R2. Juniper Networks Junos OS Evolved on on QFX5220, and PTX10003 series: 19.2-EVO versions; 19.3-EVO versions; 19.4-EVO versions prior to 19.4R2-EVO. This issue does not affect Junos OS versions prior to 19.2R1. This issue does not affect Junos OS Evolved versions prior to 19.2R1-EVO. **CVE ID : CVE-2020-1638**		
mx10000					
Improper Input Validation	09-04-2020	3.3	Due to a new NDP proxy feature for EVPN leaf nodes introduced in Junos OS 17.4, crafted NDPv6 packets could transit a Junos device configured as a Broadband Network Gateway (BNG) and reach the EVPN leaf node, causing a stale MAC address entry. This could cause legitimate traffic to be discarded, leading to a Denial of Service (DoS) condition. This issue only affects Junos OS 17.4 and later releases. Prior	https://kb.juniper.net/JSA11012	H-JUN-MX10-270420/899

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			releases do not support this feature and are unaffected by this vulnerability. This issue only affects IPv6. IPv4 ARP proxy is unaffected by this vulnerability. This issue affects Juniper Networks Junos OS: 17.4 versions prior to 17.4R2-S9, 17.4R3 on MX Series; 18.1 versions prior to 18.1R3-S9 on MX Series; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D33, 18.2X75-D411, 18.2X75-D420, 18.2X75-D60 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3 on MX Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S2, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2 on MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series. **CVE ID : CVE-2020-1633**		
srx110					
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec	https://kb.juniper.net/JSA10996	H-JUN-SRX1-270420/900

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
srx1400					
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec	https://kb.juniper.net/JSA10996	H-JUN-SRX1-270420/901

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
srx1500					
Improper Input Validation	08-04-2020	4.3	On High-End SRX Series devices, in specific configurations and when specific networking events or operator actions	N/A	H-JUN-SRX1-270420/902

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			occur, an SPC receiving genuine multicast traffic may core. Subsequently, all FPCs in a chassis may reset causing a Denial of Service. This issue affects both IPv4 and IPv6. This issue affects: Juniper Networks Junos OS 12.3X48 version 12.3X48-D80 and later versions prior to 12.3X48-D95 on High-End SRX Series. This issue does not affect Branch SRX Series devices. **CVE ID : CVE-2020-1634**		
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session	https://kb.juniper.net/JSA10996	H-JUN-SRX1-270420/903

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
srx210					
Improper Input	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation	https://kb.juniper.net/J	H-JUN-SRX2-270420/904

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions	SA10996	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
srx220					
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the	https://kb.juniper.net/JSA10996	H-JUN-SRX2-270420/905

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
srx240					
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110;	https://kb.juniper.net/JSA10996	H-JUN-SRX2-270420/906

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
srx300					
Improper Input Validation	08-04-2020	4.3	On High-End SRX Series devices, in specific configurations and when specific networking events or operator actions occur, an SPC receiving genuine multicast traffic may core. Subsequently, all FPCs in a chassis may reset causing a Denial of Service. This issue affects both IPv4 and IPv6. This issue affects: Juniper Networks Junos OS 12.3X48 version 12.3X48-D80 and later versions prior to 12.3X48-D95 on High-End SRX Series. This	N/A	H-JUN-SRX3-270420/907

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue does not affect Branch SRX Series devices. **CVE ID : CVE-2020-1634**		
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series;	https://kb.juniper.net/JSA10996	H-JUN-SRX3-270420/908

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
srx320					
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec	https://kb.juniper.net/JSA10996	H-JUN-SRX3-270420/909

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
srx340					
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior	https://kb.juniper.net/JSA10996	H-JUN-SRX3-270420/910

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
srx3400					
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is	https://kb.juniper.net/JSA10996	H-JUN-SRX3-270420/911

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
srx345					
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on	https://kb.juniper.net/JSA10996	H-JUN-SRX3-270420/912

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
srx3600					
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP	https://kb.juniper.net/JSA10996	H-JUN-SRX3-270420/913

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75		

CVSS Scoring Scale	0-1	1-2	2-3	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 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
srx4100					
Improper Input Validation	08-04-2020	4.3	On High-End SRX Series devices, in specific configurations and when specific networking events or operator actions occur, an SPC receiving genuine multicast traffic may core. Subsequently, all FPCs in a chassis may reset causing a Denial of Service. This issue affects both IPv4 and IPv6. This issue affects: Juniper Networks Junos OS 12.3X48 version 12.3X48-D80 and later versions prior to 12.3X48-D95 on High-End SRX Series. This issue does not affect Branch SRX Series devices. **CVE ID : CVE-2020-1634**	N/A	H-JUN-SRX4-270420/914
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session	https://kb.juniper.net/JSA10996	H-JUN-SRX4-270420/915

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
srx4200					
Improper Input Validation	08-04-2020	4.3	On High-End SRX Series devices, in specific configurations and when specific networking events or operator actions occur, an SPC receiving genuine multicast traffic may core. Subsequently, all FPCs in a chassis may reset causing a Denial of Service. This issue affects both IPv4 and IPv6. This issue affects: Juniper Networks Junos OS 12.3X48 version 12.3X48-D80 and later versions prior to 12.3X48-D95 on High-End SRX Series. This issue does not affect Branch SRX Series devices. **CVE ID : CVE-2020-1634**	N/A	H-JUN-SRX4-270420/916
Improper Input	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper	https://kb.juniper.net/J	H-JUN-SRX4-270420/917

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on	SA10996	

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
srx5400					
Improper Input Validation	08-04-2020	4.3	On High-End SRX Series devices, in specific configurations and when specific networking events or operator actions occur, an SPC receiving genuine multicast traffic may core. Subsequently, all FPCs in a chassis may reset causing a Denial of Service. This issue affects both IPv4 and IPv6. This issue affects: Juniper Networks Junos OS 12.3X48 version 12.3X48-D80 and later versions prior to 12.3X48-D95 on High-End SRX Series. This issue does not affect Branch SRX Series devices. **CVE ID : CVE-2020-1634**	N/A	H-JUN-SRX5-270420/918

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to	https://kb.juniper.net/JSA10996	H-JUN-SRX5-270420/919

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
srx550					
Improper Input Validation	08-04-2020	4.3	On High-End SRX Series devices, in specific configurations and when specific networking events or operator actions occur, an SPC receiving genuine multicast traffic may core. Subsequently, all FPCs in a chassis may reset causing a Denial of Service. This issue affects both IPv4 and IPv6. This issue affects: Juniper Networks Junos OS 12.3X48 version 12.3X48-D80 and later versions prior to 12.3X48-D95 on High-End SRX Series. This issue does not affect	N/A	H-JUN-SRX5-270420/920

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Branch SRX Series devices. **CVE ID : CVE-2020-1634**		
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to	https://kb.juniper.net/JSA10996	H-JUN-SRX5-270420/921

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
srx5600					
Improper Input Validation	08-04-2020	4.3	On High-End SRX Series devices, in specific configurations and when specific networking events or operator actions occur, an SPC receiving genuine multicast traffic may core. Subsequently, all FPCs in a chassis may reset causing a Denial of Service. This issue affects both IPv4 and IPv6. This issue affects: Juniper Networks Junos OS 12.3X48 version 12.3X48-D80 and later versions	N/A	H-JUN-SRX5-270420/922

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 12.3X48-D95 on High-End SRX Series. This issue does not affect Branch SRX Series devices. **CVE ID : CVE-2020-1634**		
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49	https://kb.juniper.net/JSA10996	H-JUN-SRX5-270420/923

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
srx5800					
Improper Input Validation	08-04-2020	4.3	On High-End SRX Series devices, in specific configurations and when specific networking events or operator actions occur, an SPC receiving genuine multicast traffic may core. Subsequently, all FPCs in a chassis may reset causing a Denial of Service. This issue affects both IPv4 and IPv6. This issue affects: Juniper	N/A	H-JUN-SRX5-270420/924

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS 12.3X48 version 12.3X48-D80 and later versions prior to 12.3X48-D95 on High-End SRX Series. This issue does not affect Branch SRX Series devices. **CVE ID : CVE-2020-1634**		
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1	https://kb.juniper.net/JSA10996	H-JUN-SRX5-270420/925

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
srx650					
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message	https://kb.juniper.net/JSA10996	H-JUN-SRX6-270420/926

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
ex4300					
Improper Authentication	08-04-2020	6.9	On Juniper Networks EX and QFX Series, an authentication bypass vulnerability may allow a user connected to the console port to login as root without any password. This issue might only occur in certain scenarios: • At the first reboot after performing device factory reset using the command "request system zeroize"; or • A temporary moment during the first reboot after the software upgrade when the device configured in Virtual Chassis mode. This issue affects Juniper Networks Junos OS on EX and QFX Series: 14.1X53 versions prior to 14.1X53-D53; 15.1 versions prior to 15.1R7-S4; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S4; 17.1	https://kb.juniper.net/JSA11001	H-JUN-EX43-270420/927

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 17.1R2-S11, 17.1R3-S1; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S6; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S8; 18.2 versions prior to 18.2R2; 18.3 versions prior to 18.3R1-S7, 18.3R2. This issue does not affect Juniper Networks Junos OS 12.3. **CVE ID : CVE-2020-1618**		
Information Exposure	08-04-2020	5	Juniper Networks Junos OS uses the 128.0.0.0/2 subnet for internal communications between the RE and PFEs. It was discovered that packets utilizing these IP addresses may egress an EX4300 switch, leaking configuration information such as heartbeats, kernel versions, etc. out to the Internet, leading to an information exposure vulnerability. This issue affects Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D53 on EX4300; 15.1 versions prior to 15.1R7-S6 on EX4300; 15.1X49 versions prior to 15.1X49-D200, 15.1X49-D210 on EX4300; 16.1 versions prior to 16.1R7-S7 on EX4300; 17.1 versions	https://kb.juniper.net/JSA11008	H-JUN-EX43-270420/928

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 17.1R2-S11, 17.1R3-S2 on EX4300; 17.2 versions prior to 17.2R3-S3 on EX4300; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7 on EX4300; 17.4 versions prior to 17.4R2-S9, 17.4R3 on EX4300; 18.1 versions prior to 18.1R3-S8 on EX4300; 18.2 versions prior to 18.2R3-S2 on EX4300; 18.3 versions prior to 18.3R2-S3, 18.3R3, 18.3R3-S1 on EX4300; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R3 on EX4300; 19.1 versions prior to 19.1R1-S4, 19.1R2 on EX4300; 19.2 versions prior to 19.2R1-S4, 19.2R2 on EX4300; 19.3 versions prior to 19.3R1-S1, 19.3R2 on EX4300. **CVE ID : CVE-2020-1628**		
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent	https://kb.juniper.net/JSA10996	H-JUN-EX43-270420/929

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
ex4600					
Improper Authentication	08-04-2020	6.9	On Juniper Networks EX and QFX Series, an authentication bypass vulnerability may allow a user connected to the console port to login as root without any password. This issue might only occur in certain scenarios: • At the first reboot after performing device factory reset using the command "request system zeroize"; or • A temporary moment during the first reboot after the software upgrade when the device configured in Virtual Chassis mode. This issue affects Juniper Networks Junos OS on EX and QFX Series: 14.1X53 versions prior to 14.1X53-D53; 15.1 versions prior to 15.1R7-S4; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S4; 17.1 versions prior to 17.1R2-S11, 17.1R3-S1; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to	https://kb.juniper.net/JSA11001	H-JUN-EX46-270420/930

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			17.3R2-S5, 17.3R3-S6; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S8; 18.2 versions prior to 18.2R2; 18.3 versions prior to 18.3R1-S7, 18.3R2. This issue does not affect Juniper Networks Junos OS 12.3. **CVE ID : CVE-2020-1618**		
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48	https://kb.juniper.net/JSA10996	H-JUN-EX46-270420/931

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
qfx3500					
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec	https://kb.juniper.net/JSA10996	H-JUN-QFX3-270420/932

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
qfx3600					
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec	https://kb.juniper.net/JSA10996	H-JUN-QFX3-270420/933

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
qfx5100					
Improper Authentication	08-04-2020	6.9	On Juniper Networks EX and QFX Series, an authentication bypass vulnerability may allow a user connected to the	https://kb.juniper.net/JSA11001	H-JUN-QFX5-270420/934

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			console port to login as root without any password. This issue might only occur in certain scenarios: • At the first reboot after performing device factory reset using the command "request system zeroize"; or • A temporary moment during the first reboot after the software upgrade when the device configured in Virtual Chassis mode. This issue affects Juniper Networks Junos OS on EX and QFX Series: 14.1X53 versions prior to 14.1X53-D53; 15.1 versions prior to 15.1R7-S4; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S4; 17.1 versions prior to 17.1R2-S11, 17.1R3-S1; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S6; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S8; 18.2 versions prior to 18.2R2; 18.3 versions prior to 18.3R1-S7, 18.3R2. This issue does not affect Juniper Networks Junos OS 12.3. **CVE ID : CVE-2020-1618**		
Improper Input	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation	https://kb.juniper.net/J	H-JUN-QFX5-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions	SA10996	270420/935

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
ex2300					
Improper Authentication	08-04-2020	6.9	On Juniper Networks EX and QFX Series, an authentication bypass vulnerability may allow a user connected to the console port to login as root without any password. This issue might only occur in certain scenarios: • At the first reboot after performing device factory reset using the command "request system zeroize"; or • A temporary moment during the first reboot after the software upgrade when the device configured in Virtual Chassis mode. This issue affects Juniper Networks	https://kb.juniper.net/JSA11001	H-JUN-EX23-270420/936

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Junos OS on EX and QFX Series: 14.1X53 versions prior to 14.1X53-D53; 15.1 versions prior to 15.1R7-S4; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S4; 17.1 versions prior to 17.1R2-S11, 17.1R3-S1; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S6; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S8; 18.2 versions prior to 18.2R2; 18.3 versions prior to 18.3R1-S7, 18.3R2. This issue does not affect Juniper Networks Junos OS 12.3. **CVE ID : CVE-2020-1618**		
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received	https://kb.juniper.net/JSA10996	H-JUN-EX23-270420/937

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
ex3400					
Improper Authentication	08-04-2020	6.9	On Juniper Networks EX and QFX Series, an authentication bypass vulnerability may allow a user connected to the console port to login as root without any password. This issue might only occur in certain scenarios: • At the first reboot after performing device factory reset using the command "request system zeroize"; or • A temporary moment during the first reboot after the software upgrade when the device configured in Virtual Chassis mode. This issue affects Juniper Networks Junos OS on EX and QFX Series: 14.1X53 versions prior to 14.1X53-D53; 15.1 versions prior to 15.1R7-S4; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S4; 17.1 versions prior to 17.1R2-S11, 17.1R3-S1; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S6; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-	https://kb.juniper.net/JSA11001	H-JUN-EX34-270420/938

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S8; 18.2 versions prior to 18.2R2; 18.3 versions prior to 18.3R1-S7, 18.3R2. This issue does not affect Juniper Networks Junos OS 12.3. **CVE ID : CVE-2020-1618**		
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior	https://kb.juniper.net/JSA10996	H-JUN-EX34-270420/939

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
ex2300-c					
Improper Authentication	08-04-2020	6.9	On Juniper Networks EX and QFX Series, an authentication bypass vulnerability may allow a user connected to the console port to login as root without any password. This issue might only occur in certain scenarios: • At the first reboot after performing device factory	https://kb.juniper.net/JSA11001	H-JUN-EX23-270420/940

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reset using the command "request system zeroize"; or • A temporary moment during the first reboot after the software upgrade when the device configured in Virtual Chassis mode. This issue affects Juniper Networks Junos OS on EX and QFX Series: 14.1X53 versions prior to 14.1X53-D53; 15.1 versions prior to 15.1R7-S4; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S4; 17.1 versions prior to 17.1R2-S11, 17.1R3-S1; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S6; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S8; 18.2 versions prior to 18.2R2; 18.3 versions prior to 18.3R1-S7, 18.3R2. This issue does not affect Juniper Networks Junos OS 12.3. **CVE ID : CVE-2020-1618**		
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP	https://kb.juniper.net/JSA10996	H-JUN-EX23-270420/941

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75		

CVSS Scoring Scale	0-1	1-2	2-3	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 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
ex4650					
Improper Authentication	08-04-2020	6.9	On Juniper Networks EX and QFX Series, an authentication bypass vulnerability may allow a user connected to the console port to login as root without any password. This issue might only occur in certain scenarios: • At the first reboot after performing device factory reset using the command "request system zeroize"; or • A temporary moment during the first reboot after the software upgrade when the device configured in Virtual Chassis mode. This issue affects Juniper Networks Junos OS on EX and QFX Series: 14.1X53 versions prior to 14.1X53-D53; 15.1 versions prior to 15.1R7-S4; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior	https://kb.juniper.net/JSA11001	H-JUN-EX46-270420/942

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to 16.1R7-S4; 17.1 versions prior to 17.1R2-S11, 17.1R3-S1; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S6; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S8; 18.2 versions prior to 18.2R2; 18.3 versions prior to 18.3R1-S7, 18.3R2. This issue does not affect Juniper Networks Junos OS 12.3. **CVE ID : CVE-2020-1618**		
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream.	https://kb.juniper.net/JSA10996	H-JUN-EX46-270420/943

CVSS Scoring Scale	0-1	1-2	2-3	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 affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
qfx5110					
Improper Authentication	08-04-2020	6.9	On Juniper Networks EX and QFX Series, an authentication bypass	https://kb.juniper.net/JSA11001	H-JUN-QFX5-270420/944

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability may allow a user connected to the console port to login as root without any password. This issue might only occur in certain scenarios: • At the first reboot after performing device factory reset using the command "request system zeroize"; or • A temporary moment during the first reboot after the software upgrade when the device configured in Virtual Chassis mode. This issue affects Juniper Networks Junos OS on EX and QFX Series: 14.1X53 versions prior to 14.1X53-D53; 15.1 versions prior to 15.1R7-S4; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S4; 17.1 versions prior to 17.1R2-S11, 17.1R3-S1; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S6; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S8; 18.2 versions prior to 18.2R2; 18.3 versions prior to 18.3R1-S7, 18.3R2. This issue does not affect Juniper Networks Junos OS 12.3. **CVE ID : CVE-2020-1618**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to	https://kb.juniper.net/JSA10996	H-JUN-QFX5-270420/945

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
qfx5120					
Improper Authentication	08-04-2020	6.9	On Juniper Networks EX and QFX Series, an authentication bypass vulnerability may allow a user connected to the console port to login as root without any password. This issue might only occur in certain scenarios: • At the first reboot after performing device factory reset using the command "request system zeroize"; or • A temporary moment during the first reboot after the software upgrade when the device configured in Virtual	https://kb.juniper.net/JSA11001	H-JUN-QFX5-270420/946

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Chassis mode. This issue affects Juniper Networks Junos OS on EX and QFX Series: 14.1X53 versions prior to 14.1X53-D53; 15.1 versions prior to 15.1R7-S4; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S4; 17.1 versions prior to 17.1R2-S11, 17.1R3-S1; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S6; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S8; 18.2 versions prior to 18.2R2; 18.3 versions prior to 18.3R1-S7, 18.3R2. This issue does not affect Juniper Networks Junos OS 12.3. **CVE ID : CVE-2020-1618**		
qfx5200					
Improper Authentication	08-04-2020	6.9	On Juniper Networks EX and QFX Series, an authentication bypass vulnerability may allow a user connected to the console port to login as root without any password. This issue might only occur in certain scenarios: • At the first reboot after performing device factory reset using the command "request system zeroize";	https://kb.juniper.net/JSA11001	H-JUN-QFX5-270420/947

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			or • A temporary moment during the first reboot after the software upgrade when the device configured in Virtual Chassis mode. This issue affects Juniper Networks Junos OS on EX and QFX Series: 14.1X53 versions prior to 14.1X53-D53; 15.1 versions prior to 15.1R7-S4; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S4; 17.1 versions prior to 17.1R2-S11, 17.1R3-S1; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S6; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S8; 18.2 versions prior to 18.2R2; 18.3 versions prior to 18.3R1-S7, 18.3R2. This issue does not affect Juniper Networks Junos OS 12.3. **CVE ID : CVE-2020-1618**		
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an	https://kb.juniper.net/JSA10996	H-JUN-QFX5-270420/948

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110,		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
qfx5210					
Improper Authentication	08-04-2020	6.9	On Juniper Networks EX and QFX Series, an authentication bypass vulnerability may allow a user connected to the console port to login as root without any password. This issue might only occur in certain scenarios: • At the first reboot after performing device factory reset using the command "request system zeroize"; or • A temporary moment during the first reboot after the software upgrade when the device configured in Virtual Chassis mode. This issue affects Juniper Networks Junos OS on EX and QFX Series: 14.1X53 versions prior to 14.1X53-D53; 15.1 versions prior to 15.1R7-S4; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S4; 17.1 versions prior to 17.1R2-	https://kb.juniper.net/JSA11001	H-JUN-QFX5-270420/949

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S11, 17.1R3-S1; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S6; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S8; 18.2 versions prior to 18.2R2; 18.3 versions prior to 18.3R1-S7, 18.3R2. This issue does not affect Juniper Networks Junos OS 12.3. **CVE ID : CVE-2020-1618**		
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec	https://kb.juniper.net/JSA10996	H-JUN-QFX5-270420/950

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
qfx10002					
Improper Authentication	08-04-2020	6.9	On Juniper Networks EX and QFX Series, an authentication bypass vulnerability may allow a user connected to the	https://kb.juniper.net/JSA11001	H-JUN-QFX1-270420/951

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			console port to login as root without any password. This issue might only occur in certain scenarios: • At the first reboot after performing device factory reset using the command "request system zeroize"; or • A temporary moment during the first reboot after the software upgrade when the device configured in Virtual Chassis mode. This issue affects Juniper Networks Junos OS on EX and QFX Series: 14.1X53 versions prior to 14.1X53-D53; 15.1 versions prior to 15.1R7-S4; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S4; 17.1 versions prior to 17.1R2-S11, 17.1R3-S1; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S6; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S8; 18.2 versions prior to 18.2R2; 18.3 versions prior to 18.3R1-S7, 18.3R2. This issue does not affect Juniper Networks Junos OS 12.3. **CVE ID : CVE-2020-1618**		
Improper Input	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation	https://kb.juniper.net/J	H-JUN-QFX1-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions	SA10996	270420/952

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
qfx10008					
Improper Authentication	08-04-2020	6.9	On Juniper Networks EX and QFX Series, an authentication bypass vulnerability may allow a user connected to the console port to login as root without any password. This issue might only occur in certain scenarios: • At the first reboot after performing device factory reset using the command "request system zeroize"; or • A temporary moment during the first reboot after the software upgrade when the device configured in Virtual Chassis mode. This issue affects Juniper Networks	https://kb.juniper.net/JSA11001	H-JUN-QFX1-270420/953

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Junos OS on EX and QFX Series: 14.1X53 versions prior to 14.1X53-D53; 15.1 versions prior to 15.1R7-S4; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S4; 17.1 versions prior to 17.1R2-S11, 17.1R3-S1; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S6; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S8; 18.2 versions prior to 18.2R2; 18.3 versions prior to 18.3R1-S7, 18.3R2. This issue does not affect Juniper Networks Junos OS 12.3. **CVE ID : CVE-2020-1618**		
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received	https://kb.juniper.net/JSA10996	H-JUN-QFX1-270420/954

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
Improper Initialization	08-04-2020	7.8	This issue occurs on Juniper Networks Junos OS devices which do not support Advanced Forwarding Interface (AFI) / Advanced Forwarding Toolkit (AFT). Devices using AFI and AFT are not exploitable to this issue. An improper initialization of memory in the packet forwarding architecture in Juniper Networks Junos OS non-AFI/AFT platforms which may lead to a Denial of Service (DoS) vulnerability being exploited when a genuine packet is received and inspected by non-AFT/AFI sFlow and when the device is also configured with firewall policers. This first genuine packet received and inspected by sampled flow (sFlow) through a specific firewall policer will cause the device to reboot. After the reboot has completed, if the device receives and sFlow inspects another genuine packet seen through a specific firewall policer, the device will generate a core file and reboot. Continued inspection of	N/A	H-JUN-QFX1-270420/955

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			these genuine packets will create an extended Denial of Service (DoS) condition. Depending on the method for service restoration, e.g. hard boot or soft reboot, a core file may or may not be generated the next time the packet is received and inspected by sFlow. This issue affects: Juniper Networks Junos OS 17.4 versions prior to 17.4R2-S9, 17.4R3 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.1 versions prior to 18.1R3-S9 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.2X75 versions prior to 18.2X75-D12, 18.2X75-D30 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.2 versions prior to 18.2R3 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.3 versions prior to 18.3R3 on PTX1000 and PTX10000 Series, QFX10000 Series. This issue is not applicable to Junos OS versions before 17.4R1. This issue is not applicable to Junos OS Evolved or Junos OS with Advanced Forwarding Toolkit (AFT) forwarding		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			implementations which use a different implementation of sFlow. The following example information is unrelated to this issue and is provided solely to assist you with determining if you have AFT or not. Example: A Junos OS device which supports the use of EVPN signaled VPWS with Flexible Cross Connect uses the AFT implementation. Since this configuration requires support and use of the AFT implementation to support this configuration, the device is not vulnerable to this issue as the sFlow implementation is different using the AFT architecture. For further details about AFT visit the AFI / AFT are in the links below. If you are uncertain if you use the AFI/AFT implementation or not, there are configuration examples in the links below which you may use to determine if you are vulnerable to this issue or not. If the commands work, you are. If not, you are not. You may also use the Feature Explorer to determine if		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AFI/AFT is supported or not. If you are still uncertain, please contact your support resources. **CVE ID : CVE-2020-1617**		
qfx10016					
Improper Authentication	08-04-2020	6.9	On Juniper Networks EX and QFX Series, an authentication bypass vulnerability may allow a user connected to the console port to login as root without any password. This issue might only occur in certain scenarios: • At the first reboot after performing device factory reset using the command "request system zeroize"; or • A temporary moment during the first reboot after the software upgrade when the device configured in Virtual Chassis mode. This issue affects Juniper Networks Junos OS on EX and QFX Series: 14.1X53 versions prior to 14.1X53-D53; 15.1 versions prior to 15.1R7-S4; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S4; 17.1 versions prior to 17.1R2-S11, 17.1R3-S1; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S6;	https://kb.juniper.net/JSA11001	H-JUN-QFX1-270420/956

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S8; 18.2 versions prior to 18.2R2; 18.3 versions prior to 18.3R1-S7, 18.3R2. This issue does not affect Juniper Networks Junos OS 12.3. **CVE ID : CVE-2020-1618**		
Improper Input Validation	08-04-2020	5	A vulnerability in the BGP FlowSpec implementation may cause a Juniper Networks Junos OS device to terminate an established BGP session upon receiving a specific BGP FlowSpec advertisement. The BGP NOTIFICATION message that terminates an established BGP session is sent toward the peer device that originally sent the specific BGP FlowSpec advertisement. This specific BGP FlowSpec advertisement received from a BGP peer might get propagated from a Junos OS device running the fixed release to another device that is vulnerable causing BGP session termination downstream. This issue affects IPv4 and IPv6 BGP FlowSpec deployment. This issue affects Juniper Networks Junos OS: 12.3; 12.3X48 on SRX Series; 14.1X53 on	https://kb.juniper.net/JSA10996	H-JUN-QFX1-270420/957

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EX and QFX Series; 15.1 versions prior to 15.1R7-S5; 15.1F versions prior to 15.1F6-S13; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238 on QFX5200/QFX5110; 15.1X53 versions prior to 15.1X53-D497 on NFX Series; 15.1X53 versions prior to 15.1X53-D592 on EX2300/EX3400; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S12, 17.1R3; 17.2 versions prior to 17.2R2-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D102, 17.2X75-D110, 17.2X75-D44; 17.3 versions prior to 17.3R2-S5, 17.3R3-S5; 17.4 versions prior to 17.4R1-S8, 17.4R2; 18.1 versions prior to 18.1R2-S4, 18.1R3; 18.2X75 versions prior to 18.2X75-D20. **CVE ID : CVE-2020-1613**		
Improper Initialization	08-04-2020	7.8	This issue occurs on Juniper Networks Junos OS devices which do not support Advanced Forwarding Interface (AFI) / Advanced Forwarding Toolkit (AFT). Devices using AFI and AFT are not exploitable to this issue. An improper initialization	N/A	H-JUN-QFX1-270420/958

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of memory in the packet forwarding architecture in Juniper Networks Junos OS non-AFI/AFT platforms which may lead to a Denial of Service (DoS) vulnerability being exploited when a genuine packet is received and inspected by non-AFT/AFI sFlow and when the device is also configured with firewall policers. This first genuine packet received and inspected by sampled flow (sFlow) through a specific firewall policer will cause the device to reboot. After the reboot has completed, if the device receives and sFlow inspects another genuine packet seen through a specific firewall policer, the device will generate a core file and reboot. Continued inspection of these genuine packets will create an extended Denial of Service (DoS) condition. Depending on the method for service restoration, e.g. hard boot or soft reboot, a core file may or may not be generated the next time the packet is received and inspected by sFlow. This issue affects: Juniper Networks Junos OS 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 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.1 versions prior to 18.1R3-S9 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.2X75 versions prior to 18.2X75-D12, 18.2X75-D30 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.2 versions prior to 18.2R3 on PTX1000 and PTX10000 Series, QFX10000 Series; 18.3 versions prior to 18.3R3 on PTX1000 and PTX10000 Series, QFX10000 Series. This issue is not applicable to Junos OS versions before 17.4R1. This issue is not applicable to Junos OS Evolved or Junos OS with Advanced Forwarding Toolkit (AFT) forwarding implementations which use a different implementation of sFlow. The following example information is unrelated to this issue and is provided solely to assist you with determining if you have AFT or not. Example: A Junos OS device which supports the use of EVPN signaled VPWS with Flexible Cross		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connect uses the AFT implementation. Since this configuration requires support and use of the AFT implementation to support this configuration, the device is not vulnerable to this issue as the sFlow implementation is different using the AFT architecture. For further details about AFT visit the AFI / AFT are in the links below. If you are uncertain if you use the AFI/AFT implementation or not, there are configuration examples in the links below which you may use to determine if you are vulnerable to this issue or not. If the commands work, you are. If not, you are not. You may also use the Feature Explorer to determine if AFI/AFT is supported or not. If you are still uncertain, please contact your support resources. **CVE ID : CVE-2020-1617**		
mx10					
Improper Input Validation	09-04-2020	3.3	Due to a new NDP proxy feature for EVPN leaf nodes introduced in Junos OS 17.4, crafted NDPv6 packets could transit a Junos device configured	https://kb.juniper.net/JSA11012	H-JUN-MX10-270420/959

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			as a Broadband Network Gateway (BNG) and reach the EVPN leaf node, causing a stale MAC address entry. This could cause legitimate traffic to be discarded, leading to a Denial of Service (DoS) condition. This issue only affects Junos OS 17.4 and later releases. Prior releases do not support this feature and are unaffected by this vulnerability. This issue only affects IPv6. IPv4 ARP proxy is unaffected by this vulnerability. This issue affects Juniper Networks Junos OS: 17.4 versions prior to 17.4R2-S9, 17.4R3 on MX Series; 18.1 versions prior to 18.1R3-S9 on MX Series; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D33, 18.2X75-D411, 18.2X75-D420, 18.2X75-D60 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3 on MX Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S2, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2 on MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series.		

CVSS Scoring Scale	0-1	1-2	2-3	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-2020-1633		
mx10003					
Improper Input Validation	09-04-2020	3.3	Due to a new NDP proxy feature for EVPN leaf nodes introduced in Junos OS 17.4, crafted NDPv6 packets could transit a Junos device configured as a Broadband Network Gateway (BNG) and reach the EVPN leaf node, causing a stale MAC address entry. This could cause legitimate traffic to be discarded, leading to a Denial of Service (DoS) condition. This issue only affects Junos OS 17.4 and later releases. Prior releases do not support this feature and are unaffected by this vulnerability. This issue only affects IPv6. IPv4 ARP proxy is unaffected by this vulnerability. This issue affects Juniper Networks Junos OS: 17.4 versions prior to 17.4R2-S9, 17.4R3 on MX Series; 18.1 versions prior to 18.1R3-S9 on MX Series; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D33, 18.2X75-D411, 18.2X75-D420, 18.2X75-D60 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3 on	https://kb.juniper.net/JSA11012	H-JUN-MX10-270420/960

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MX Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S2, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2 on MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series. **CVE ID : CVE-2020-1633**		
Improper Input Validation	08-04-2020	5	The FPC (Flexible PIC Concentrator) of Juniper Networks Junos OS and Junos OS Evolved may restart after processing a specific IPv4 packet. Only packets destined to the device itself, successfully reaching the RE through existing edge and control plane filtering, will be able to cause the FPC restart. When this issue occurs, all traffic via the FPC will be dropped. By continuously sending this specific IPv4 packet, an attacker can repeatedly crash the FPC, causing an extended Denial of Service (DoS) condition. This issue can only occur when processing a specific IPv4 packet. IPv6 packets cannot trigger this issue. This issue affects: Juniper Networks Junos OS on MX Series with MPC10E or MPC11E and PTX10001: 19.2 versions prior to 19.2R1-S4, 19.2R2; 19.3 versions	https://kb.juniper.net/JSA11019	H-JUN-MX10-270420/961

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.3R2-S2, 19.3R3; 19.4 versions prior to 19.4R1-S1, 19.4R2. Juniper Networks Junos OS Evolved on on QFX5220, and PTX10003 series: 19.2-EVO versions; 19.3-EVO versions; 19.4-EVO versions prior to 19.4R2-EVO. This issue does not affect Junos OS versions prior to 19.2R1. This issue does not affect Junos OS Evolved versions prior to 19.2R1-EVO. **CVE ID : CVE-2020-1638**		
mx104					
Improper Input Validation	09-04-2020	3.3	Due to a new NDP proxy feature for EVPN leaf nodes introduced in Junos OS 17.4, crafted NDPv6 packets could transit a Junos device configured as a Broadband Network Gateway (BNG) and reach the EVPN leaf node, causing a stale MAC address entry. This could cause legitimate traffic to be discarded, leading to a Denial of Service (DoS) condition. This issue only affects Junos OS 17.4 and later releases. Prior releases do not support this feature and are unaffected by this vulnerability. This issue only affects IPv6. IPv4 ARP proxy is unaffected	https://kb.juniper.net/JSA11012	H-JUN-MX10-270420/962

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			by this vulnerability. This issue affects Juniper Networks Junos OS: 17.4 versions prior to 17.4R2-S9, 17.4R3 on MX Series; 18.1 versions prior to 18.1R3-S9 on MX Series; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D33, 18.2X75-D411, 18.2X75-D420, 18.2X75-D60 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3 on MX Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S2, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2 on MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series. **CVE ID : CVE-2020-1633**		
mx150					
Improper Input Validation	08-04-2020	5	A vulnerability in Juniper Networks Junos OS on vMX and MX150 devices may allow an attacker to cause a Denial of Service (DoS) by sending specific packets requiring special processing in microcode that the flow cache can't handle, causing the riot forwarding daemon to crash. By continuously sending the same specific packets, an attacker can	https://kb.juniper.net/JSA11006	H-JUN-MX15-270420/963

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			repeatedly crash the riot process causing a sustained Denial of Service. Flow cache is specific to vMX based products and the MX150, and is enabled by default in performance mode. This issue can only be triggered by traffic destined to the device. Transit traffic will not cause the riot daemon to crash. When the issue occurs, a core dump and riot log file entry are generated. For example: /var/crash/core.J-UKERN.mpc0.1557255993.3864.gz /home/pfe/RIOT logs: fpc0 riot[1888]: PANIC in lu_reorder_send_packet_postproc(): fpc0 riot[6655]: PANIC in lu_reorder_send_packet_postproc(): This issue affects Juniper Networks Junos OS: 18.1 versions prior to 18.1R3 on vMX and MX150; 18.2 versions prior to 18.2R3 on vMX and MX150; 18.2X75 versions prior to 18.2X75-D60 on vMX and MX150; 18.3 versions prior to 18.3R3 on vMX and MX150; 18.4 versions prior to 18.4R2 on vMX and MX150; 19.1 versions prior to 19.1R2 on vMX		

CVSS Scoring Scale	0-1	1-2	2-3	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 MX150. This issue does not affect Junos OS versions prior to 18.1R1. **CVE ID : CVE-2020-1627**		
Improper Input Validation	09-04-2020	3.3	Due to a new NDP proxy feature for EVPN leaf nodes introduced in Junos OS 17.4, crafted NDPv6 packets could transit a Junos device configured as a Broadband Network Gateway (BNG) and reach the EVPN leaf node, causing a stale MAC address entry. This could cause legitimate traffic to be discarded, leading to a Denial of Service (DoS) condition. This issue only affects Junos OS 17.4 and later releases. Prior releases do not support this feature and are unaffected by this vulnerability. This issue only affects IPv6. IPv4 ARP proxy is unaffected by this vulnerability. This issue affects Juniper Networks Junos OS: 17.4 versions prior to 17.4R2-S9, 17.4R3 on MX Series; 18.1 versions prior to 18.1R3-S9 on MX Series; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D33, 18.2X75-D411, 18.2X75-D420, 18.2X75-D60 on MX Series; 18.3	https://kb.juniper.net/JSA11012	H-JUN-MX15-270420/964

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3 on MX Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S2, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2 on MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series. **CVE ID : CVE-2020-1633**		
mx2008					
Improper Input Validation	09-04-2020	3.3	Due to a new NDP proxy feature for EVPN leaf nodes introduced in Junos OS 17.4, crafted NDPv6 packets could transit a Junos device configured as a Broadband Network Gateway (BNG) and reach the EVPN leaf node, causing a stale MAC address entry. This could cause legitimate traffic to be discarded, leading to a Denial of Service (DoS) condition. This issue only affects Junos OS 17.4 and later releases. Prior releases do not support this feature and are unaffected by this vulnerability. This issue only affects IPv6. IPv4 ARP proxy is unaffected by this vulnerability. This issue affects Juniper Networks Junos OS: 17.4 versions prior to 17.4R2-S9, 17.4R3 on MX Series;	https://kb.juniper.net/JSA11012	H-JUN-MX20-270420/965

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.1 versions prior to 18.1R3-S9 on MX Series; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D33, 18.2X75-D411, 18.2X75-D420, 18.2X75-D60 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3 on MX Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S2, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2 on MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series. **CVE ID : CVE-2020-1633**		
Improper Input Validation	08-04-2020	5	The FPC (Flexible PIC Concentrator) of Juniper Networks Junos OS and Junos OS Evolved may restart after processing a specific IPv4 packet. Only packets destined to the device itself, successfully reaching the RE through existing edge and control plane filtering, will be able to cause the FPC restart. When this issue occurs, all traffic via the FPC will be dropped. By continuously sending this specific IPv4 packet, an attacker can repeatedly crash the FPC, causing an extended Denial of Service (DoS) condition.	https://kb.juniper.net/JSA11019	H-JUN-MX20-270420/966

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This issue can only occur when processing a specific IPv4 packet. IPv6 packets cannot trigger this issue. This issue affects: Juniper Networks Junos OS on MX Series with MPC10E or MPC11E and PTX10001: 19.2 versions prior to 19.2R1-S4, 19.2R2; 19.3 versions prior to 19.3R2-S2, 19.3R3; 19.4 versions prior to 19.4R1-S1, 19.4R2. Juniper Networks Junos OS Evolved on on QFX5220, and PTX10003 series: 19.2-EVO versions; 19.3-EVO versions; 19.4-EVO versions prior to 19.4R2-EVO. This issue does not affect Junos OS versions prior to 19.2R1. This issue does not affect Junos OS Evolved versions prior to 19.2R1-EVO. **CVE ID : CVE-2020-1638**		
mx2010					
Improper Input Validation	09-04-2020	3.3	Due to a new NDP proxy feature for EVPN leaf nodes introduced in Junos OS 17.4, crafted NDPv6 packets could transit a Junos device configured as a Broadband Network Gateway (BNG) and reach the EVPN leaf node, causing a stale MAC address entry. This could cause legitimate traffic to	https://kb.juniper.net/JSA11012	H-JUN-MX20-270420/967

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			be discarded, leading to a Denial of Service (DoS) condition. This issue only affects Junos OS 17.4 and later releases. Prior releases do not support this feature and are unaffected by this vulnerability. This issue only affects IPv6. IPv4 ARP proxy is unaffected by this vulnerability. This issue affects Juniper Networks Junos OS: 17.4 versions prior to 17.4R2-S9, 17.4R3 on MX Series; 18.1 versions prior to 18.1R3-S9 on MX Series; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D33, 18.2X75-D411, 18.2X75-D420, 18.2X75-D60 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3 on MX Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S2, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2 on MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series. **CVE ID : CVE-2020-1633**		
Improper Input Validation	08-04-2020	5	The FPC (Flexible PIC Concentrator) of Juniper Networks Junos OS and Junos OS Evolved may restart after processing a	https://kb.juniper.net/JSA11019	H-JUN-MX20-270420/968

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specific IPv4 packet. Only packets destined to the device itself, successfully reaching the RE through existing edge and control plane filtering, will be able to cause the FPC restart. When this issue occurs, all traffic via the FPC will be dropped. By continuously sending this specific IPv4 packet, an attacker can repeatedly crash the FPC, causing an extended Denial of Service (DoS) condition. This issue can only occur when processing a specific IPv4 packet. IPv6 packets cannot trigger this issue. This issue affects: Juniper Networks Junos OS on MX Series with MPC10E or MPC11E and PTX10001: 19.2 versions prior to 19.2R1-S4, 19.2R2; 19.3 versions prior to 19.3R2-S2, 19.3R3; 19.4 versions prior to 19.4R1-S1, 19.4R2. Juniper Networks Junos OS Evolved on on QFX5220, and PTX10003 series: 19.2-EVO versions; 19.3-EVO versions; 19.4-EVO versions prior to 19.4R2-EVO. This issue does not affect Junos OS versions prior to 19.2R1. This issue does not affect Junos OS Evolved 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 19.2R1-EVO. **CVE ID : CVE-2020-1638**		
mi					
xiaomi_xiaoai_speaker_pro_lx06					
Improper Input Validation	08-04-2020	7.2	An issue was discovered on XIAOMI XIAOAI speaker Pro LX06 1.58.10. Attackers can activate the failsafe mode during the boot process, and use the mi_console command cascaded by the SN code shown on the product to get the root shell password, and then the attacker can (i) read Wi-Fi SSID or password, (ii) read the dialogue text files between users and XIAOMI XIAOAI speaker Pro LX06, (iii) use Text-To-Speech tools pretend XIAOMI speakers' voice achieve social engineering attacks, (iv) eavesdrop on users and record what XIAOMI XIAOAI speaker Pro LX06 hears, (v) modify system files, (vi) use commands to send any IR code through IR emitter on XIAOMI XIAOAI Speaker Pro (LX06), (vii) stop voice assistant service, (viii) enable the XIAOMI XIAOAI Speaker Pro's SSH or TELNET service as a backdoor, (IX) tamper with the router	N/A	H-MI-XIAO-270420/969

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			configuration of the router in the local area networks. **CVE ID : CVE-2020-10262**		
Improper Input Validation	08-04-2020	7.2	An issue was discovered on XIAOMI XIAOAI speaker Pro LX06 1.52.4. Attackers can get root shell by accessing the UART interface and then they can (i) read Wi-Fi SSID or password, (ii) read the dialogue text files between users and XIAOMI XIAOAI speaker Pro LX06, (iii) use Text-To-Speech tools pretend XIAOMI speakers' voice achieve social engineering attacks, (iv) eavesdrop on users and record what XIAOMI XIAOAI speaker Pro LX06 hears, (v) modify system files, (vi) use commands to send any IR code through IR emitter on XIAOMI XIAOAI Speaker Pro LX06, (vii) stop voice assistant service, (viii) enable the XIAOMI XIAOAI Speaker Pro' SSH or TELNET service as a backdoor, (IX) tamper with the router configuration of the router in the local area networks. **CVE ID : CVE-2020-10263**	N/A	H-MI-XIAO-270420/970

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mysyngeryss					
husky_rtu_6049-e70					
Improper Check for Unusual or Exceptional Conditions	14-04-2020	8.5	The Synergy Systems & Solutions (SSS) HUSKY RTU 6049-E70, with firmware Versions 5.0 and prior, has an Improper Check for Unusual or Exceptional Conditions (CWE-754) vulnerability. The affected product is vulnerable to specially crafted TCP packets, which can cause the device to shut down or reboot and lose configuration settings. This is a different issue than CVE-2019-16879, CVE-2019-20045, CVE-2019-20046, CVE-2020-7801, and CVE-2020-7802. **CVE ID : CVE-2020-7800**	N/A	H-MYS-HUSK-270420/971
Information Exposure	14-04-2020	5	The Synergy Systems & Solutions (SSS) HUSKY RTU 6049-E70, with firmware Versions 5.0 and prior, has an Exposure of Sensitive Information to an Unauthorized Actor (CWE-200) vulnerability. The affected product is vulnerable to information exposure over the SNMP protocol. This is a different issue than CVE-2019-16879, CVE-2019-20045, CVE-2019-20046,	N/A	H-MYS-HUSK-270420/972

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-7800, and CVE-2020-7802. **CVE ID : CVE-2020-7801**		
Incorrect Default Permissions	14-04-2020	5	The Synergy Systems & Solutions (SSS) HUSKY RTU 6049-E70, with firmware Versions 5.0 and prior, has an Incorrect Default Permissions (CWE-276) vulnerability. The affected product is vulnerable to insufficient default permissions, which could allow an attacker to view network configurations through SNMP communication. This is a different issue than CVE-2019-16879, CVE-2019-20045, CVE-2019-20046, CVE-2020-7800, and CVE-2020-7801. **CVE ID : CVE-2020-7802**	N/A	H-MYS-HUSK-270420/973
Paloaltonetworks					
pa-7050					
Use of Externally-Controlled Format String	08-04-2020	9.3	A format string vulnerability in the Varrcvr daemon of PAN-OS on PA-7000 Series devices with a Log Forwarding Card (LFC) allows remote attackers to crash the daemon creating a denial of service condition or potentially execute code with root privileges. This issue affects Palo Alto	N/A	H-PAL-PA-7-270420/974

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networks PAN-OS 9.0 versions before 9.0.7; PAN-OS 9.1 versions before 9.1.2 on PA-7000 Series devices with an LFC installed and configured. This issue requires WildFire services to be configured and enabled. This issue does not affect PAN-OS 8.1 and earlier releases. This issue does not affect any other PA Series firewalls. **CVE ID : CVE-2020-1992**		
pa-7080					
Use of Externally-Controlled Format String	08-04-2020	9.3	A format string vulnerability in the Varrcvr daemon of PAN-OS on PA-7000 Series devices with a Log Forwarding Card (LFC) allows remote attackers to crash the daemon creating a denial of service condition or potentially execute code with root privileges. This issue affects Palo Alto Networks PAN-OS 9.0 versions before 9.0.7; PAN-OS 9.1 versions before 9.1.2 on PA-7000 Series devices with an LFC installed and configured. This issue requires WildFire services to be configured and enabled. This issue	N/A	H-PAL-PA-7-270420/975

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			does not affect PAN-OS 8.1 and earlier releases. This issue does not affect any other PA Series firewalls. **CVE ID : CVE-2020-1992**		
plathome					
easyblocks_ipv6					
Cross-Site Request Forgery (CSRF)	08-04-2020	6.8	Cross-site request forgery (CSRF) vulnerability in EasyBlocks IPv6 Ver. 2.0.1 and earlier and Enterprise Ver. 2.0.1 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors. **CVE ID : CVE-2020-5549**	N/A	H-PLA-EASY-270420/976
Session Fixation	08-04-2020	5.8	Session fixation vulnerability in EasyBlocks IPv6 Ver. 2.0.1 and earlier, and Enterprise Ver. 2.0.1 and earlier allows remote attackers to impersonate a registered user and log in the management console, that may result in information alteration/disclosure via unspecified vectors. **CVE ID : CVE-2020-5550**	N/A	H-PLA-EASY-270420/977
easyblocks_ipv6_enterprise					
Cross-Site Request Forgery (CSRF)	08-04-2020	6.8	Cross-site request forgery (CSRF) vulnerability in EasyBlocks IPv6 Ver. 2.0.1 and earlier and Enterprise	N/A	H-PLA-EASY-270420/978

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Ver. 2.0.1 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors. **CVE ID : CVE-2020-5549**		
Session Fixation	08-04-2020	5.8	Session fixation vulnerability in EasyBlocks IPv6 Ver. 2.0.1 and earlier, and Enterprise Ver. 2.0.1 and earlier allows remote attackers to impersonate a registered user and log in the management console, that may result in information alteration/disclosure via unspecified vectors. **CVE ID : CVE-2020-5550**	N/A	H-PLA-EASY-270420/979
ST					
stm32f1					
Information Exposure	06-04-2020	5	STMicroelectronics STM32F1 devices have Incorrect Access Control. **CVE ID : CVE-2020-8004**	N/A	H-ST-STM3-270420/980
stormshield					
sn310					
URL Redirection to Untrusted Site ('Open Redirect')	13-04-2020	5.8	Stormshield Network Security 310 3.7.10 devices have an auth/lang.html?rurl= Open Redirect vulnerability on the captive portal. For example, the attacker can use rurl=//example.com	https://advisories.stormshield.eu/2020-001/	H-STO-SN31-270420/981

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			instead of rurl=https://example.com in the query string. **CVE ID : CVE-2020-8430**		
Technicolor					
tc7337					
Insufficiently Protected Credentials	01-04-2020	5	An issue was discovered on Technicolor TC7337 8.89.17 devices. An attacker can discover admin credentials in the backup file, aka backupsettings.conf. **CVE ID : CVE-2020-11449**	N/A	H-TEC-TC73-270420/982
Tp-link					
tl-wr841n					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-04-2020	9	A buffer overflow in the httpd daemon on TP-Link TL-WR841N V10 (firmware version 3.16.9) devices allows an authenticated remote attacker to execute arbitrary code via a GET request to the page for the configuration of the Wi-Fi network. **CVE ID : CVE-2020-8423**	N/A	H-TP--TL-W-270420/983
nc450					
NULL Pointer Dereference	01-04-2020	5	TP-Link NC200 through 2.1.8_Build_171109, NC210 through 1.0.9_Build_171214, NC220 through 1.3.0_Build_180105, NC230 through 1.3.0_Build_171205,	N/A	H-TP--NC45-270420/984

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NC250 through 1.3.0_Build_171205, NC260 through 1.5.1_Build_190805, and NC450 through 1.5.0_Build_181022 devices allow a remote NULL Pointer Dereference. **CVE ID : CVE-2020-10231**		
Improper Authentication	01-04-2020	5	TP-Link cloud cameras through 2020-02-09 allow remote attackers to bypass authentication and obtain sensitive information via vectors involving a Wi-Fi session with GPS enabled, aka CNVD-2020-04855. **CVE ID : CVE-2020-11445**	N/A	H-TP--NC45-270420/985
nc260					
NULL Pointer Dereference	01-04-2020	5	TP-Link NC200 through 2.1.8_Build_171109, NC210 through 1.0.9_Build_171214, NC220 through 1.3.0_Build_180105, NC230 through 1.3.0_Build_171205, NC250 through 1.3.0_Build_171205, NC260 through 1.5.1_Build_190805, and NC450 through 1.5.0_Build_181022 devices allow a remote NULL Pointer	N/A	H-TP--NC26-270420/986

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Dereference. **CVE ID : CVE-2020-10231**		
Improper Authentication	01-04-2020	5	TP-Link cloud cameras through 2020-02-09 allow remote attackers to bypass authentication and obtain sensitive information via vectors involving a Wi-Fi session with GPS enabled, aka CNVD-2020-04855. **CVE ID : CVE-2020-11445**	N/A	H-TP--NC26-270420/987
nc250					
NULL Pointer Dereference	01-04-2020	5	TP-Link NC200 through 2.1.8_Build_171109, NC210 through 1.0.9_Build_171214, NC220 through 1.3.0_Build_180105, NC230 through 1.3.0_Build_171205, NC250 through 1.3.0_Build_171205, NC260 through 1.5.1_Build_190805, and NC450 through 1.5.0_Build_181022 devices allow a remote NULL Pointer Dereference. **CVE ID : CVE-2020-10231**	N/A	H-TP--NC25-270420/988
Improper Authentication	01-04-2020	5	TP-Link cloud cameras through 2020-02-09 allow remote attackers to bypass authentication and obtain sensitive	N/A	H-TP--NC25-270420/989

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information via vectors involving a Wi-Fi session with GPS enabled, aka CNVD-2020-04855. **CVE ID : CVE-2020-11445**		
nc230					
NULL Pointer Dereference	01-04-2020	5	TP-Link NC200 through 2.1.8_Build_171109, NC210 through 1.0.9_Build_171214, NC220 through 1.3.0_Build_180105, NC230 through 1.3.0_Build_171205, NC250 through 1.3.0_Build_171205, NC260 through 1.5.1_Build_190805, and NC450 through 1.5.0_Build_181022 devices allow a remote NULL Pointer Dereference. **CVE ID : CVE-2020-10231**	N/A	H-TP--NC23-270420/990
Improper Authentication	01-04-2020	5	TP-Link cloud cameras through 2020-02-09 allow remote attackers to bypass authentication and obtain sensitive information via vectors involving a Wi-Fi session with GPS enabled, aka CNVD-2020-04855. **CVE ID : CVE-2020-11445**	N/A	H-TP--NC23-270420/991
nc220					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	01-04-2020	5	TP-Link NC200 through 2.1.8_Build_171109, NC210 through 1.0.9_Build_171214, NC220 through 1.3.0_Build_180105, NC230 through 1.3.0_Build_171205, NC250 through 1.3.0_Build_171205, NC260 through 1.5.1_Build_190805, and NC450 through 1.5.0_Build_181022 devices allow a remote NULL Pointer Dereference. **CVE ID : CVE-2020-10231**	N/A	H-TP--NC22-270420/992
Improper Authentication	01-04-2020	5	TP-Link cloud cameras through 2020-02-09 allow remote attackers to bypass authentication and obtain sensitive information via vectors involving a Wi-Fi session with GPS enabled, aka CNVD-2020-04855. **CVE ID : CVE-2020-11445**	N/A	H-TP--NC22-270420/993
nc210					
NULL Pointer Dereference	01-04-2020	5	TP-Link NC200 through 2.1.8_Build_171109, NC210 through 1.0.9_Build_171214, NC220 through 1.3.0_Build_180105, NC230 through 1.3.0_Build_171205, NC250 through	N/A	H-TP--NC21-270420/994

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.3.0_Build_171205, NC260 through 1.5.1_Build_190805, and NC450 through 1.5.0_Build_181022 devices allow a remote NULL Pointer Dereference. **CVE ID : CVE-2020-10231**		
Improper Authentication	01-04-2020	5	TP-Link cloud cameras through 2020-02-09 allow remote attackers to bypass authentication and obtain sensitive information via vectors involving a Wi-Fi session with GPS enabled, aka CNVD-2020-04855. **CVE ID : CVE-2020-11445**	N/A	H-TP--NC21-270420/995
nc200					
NULL Pointer Dereference	01-04-2020	5	TP-Link NC200 through 2.1.8_Build_171109, NC210 through 1.0.9_Build_171214, NC220 through 1.3.0_Build_180105, NC230 through 1.3.0_Build_171205, NC250 through 1.3.0_Build_171205, NC260 through 1.5.1_Build_190805, and NC450 through 1.5.0_Build_181022 devices allow a remote NULL Pointer Dereference.	N/A	H-TP--NC20-270420/996

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-10231		
Improper Authentication	01-04-2020	5	TP-Link cloud cameras through 2020-02-09 allow remote attackers to bypass authentication and obtain sensitive information via vectors involving a Wi-Fi session with GPS enabled, aka CNVD-2020-04855. **CVE ID : CVE-2020-11445**	N/A	H-TP--NC20-270420/997
kc300s2					
Improper Authentication	01-04-2020	5	TP-Link cloud cameras through 2020-02-09 allow remote attackers to bypass authentication and obtain sensitive information via vectors involving a Wi-Fi session with GPS enabled, aka CNVD-2020-04855. **CVE ID : CVE-2020-11445**	N/A	H-TP--KC30-270420/998
kc310s2					
Improper Authentication	01-04-2020	5	TP-Link cloud cameras through 2020-02-09 allow remote attackers to bypass authentication and obtain sensitive information via vectors involving a Wi-Fi session with GPS enabled, aka CNVD-2020-04855. **CVE ID : CVE-2020-11445**	N/A	H-TP--KC31-270420/999
kc200					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	01-04-2020	5	TP-Link cloud cameras through 2020-02-09 allow remote attackers to bypass authentication and obtain sensitive information via vectors involving a Wi-Fi session with GPS enabled, aka CNVD-2020-04855. **CVE ID : CVE-2020-11445**	N/A	H-TP--KC20-270420/1000
tapo_c200					
Improper Authentication	01-04-2020	5	TP-Link cloud cameras through 2020-02-09 allow remote attackers to bypass authentication and obtain sensitive information via vectors involving a Wi-Fi session with GPS enabled, aka CNVD-2020-04855. **CVE ID : CVE-2020-11445**	N/A	H-TP--TAPO-270420/1001
tapo_c100					
Improper Authentication	01-04-2020	5	TP-Link cloud cameras through 2020-02-09 allow remote attackers to bypass authentication and obtain sensitive information via vectors involving a Wi-Fi session with GPS enabled, aka CNVD-2020-04855. **CVE ID : CVE-2020-11445**	N/A	H-TP--TAPO-270420/1002
tl-sc3430					
Improper Authentication	01-04-2020	5	TP-Link cloud cameras through 2020-02-09	N/A	H-TP--TL-S-270420/1003

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow remote attackers to bypass authentication and obtain sensitive information via vectors involving a Wi-Fi session with GPS enabled, aka CNVD-2020-04855. **CVE ID : CVE-2020-11445**		
tl-sc3430n					
Improper Authentication	01-04-2020	5	TP-Link cloud cameras through 2020-02-09 allow remote attackers to bypass authentication and obtain sensitive information via vectors involving a Wi-Fi session with GPS enabled, aka CNVD-2020-04855. **CVE ID : CVE-2020-11445**	N/A	H-TP--TL-S-270420/1004
tl-sc4171g					
Improper Authentication	01-04-2020	5	TP-Link cloud cameras through 2020-02-09 allow remote attackers to bypass authentication and obtain sensitive information via vectors involving a Wi-Fi session with GPS enabled, aka CNVD-2020-04855. **CVE ID : CVE-2020-11445**	N/A	H-TP--TL-S-270420/1005
universal-robots					
ur10					
Information Exposure	06-04-2020	5.8	CB3 SW Version 3.3 and upwards, e-series SW Version 5.0 and upwards	https://www.universal-	H-UNI-UR10-270420/1006

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow authenticated access to the RTDE (Real-Time Data Exchange) interface on port 30004 which allows setting registers, the speed slider fraction as well as digital and analog Outputs. Additionally unautheticated reading of robot data is also possible **CVE ID : CVE-2020-10264**	robots.com /how-tos-and-faqs/how-to/ur-how-tos/real-time-data-exchange-rtde-guide/	
Missing Authentication for Critical Function	06-04-2020	9	Universal Robots Robot Controllers Version CB2 SW Version 1.4 upwards, CB3 SW Version 3.0 and upwards, e-series SW Version 5.0 and upwards expose a service called DashBoard server at port 29999 that allows for control over core robot functions like starting/stopping programs, shutdown, reset safety and more. The DashBoard server is not protected by any kind of authentication or authorization. **CVE ID : CVE-2020-10265**	https://www.universal-robots.com /how-tos-and-faqs/how-to/ur-how-tos/real-time-data-exchange-rtde-guide/	H-UNI-UR10-270420/1007
Insufficient Verification of Data Authenticity	06-04-2020	6.8	UR+ (Universal Robots+) is a platform of hardware and software component sellers, for Universal Robots robots. When installing any of these components in the robots	https://github.com/aliasrobotics/RVD/issues/1487	H-UNI-UR10-270420/1008

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(e.g. in the UR10), no integrity checks are performed. Moreover, the SDK for making such components can be easily obtained from Universal Robots. An attacker could exploit this flaw by crafting a custom component with the SDK, performing Person-In-The-Middle attacks (PITM) and shipping the maliciously-crafted component on demand. **CVE ID : CVE-2020-10266**		
Missing Encryption of Sensitive Data	06-04-2020	5	Universal Robots control box CB 3.1 across firmware versions (tested on 1.12.1, 1.12, 1.11 and 1.10) does not encrypt or protect in any way the intellectual property artifacts installed from the UR+ platform of hardware and software components (URCaps). These files (*.urcaps) are stored under '/root/.urcaps' as plain zip files containing all the logic to add functionality to the UR3, UR5 and UR10 robots. This flaw allows attackers with access to the robot or the robot network (while in combination with other flaws) to retrieve and easily exfiltrate all	https://github.com/aliasrobotics/RVD/issues/1489	H-UNI-UR10-270420/1009

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			installed intellectual property. **CVE ID : CVE-2020-10267**		
ur3					
Information Exposure	06-04-2020	5.8	CB3 SW Version 3.3 and upwards, e-series SW Version 5.0 and upwards allow authenticated access to the RTDE (Real-Time Data Exchange) interface on port 30004 which allows setting registers, the speed slider fraction as well as digital and analog Outputs. Additionally unautheticated reading of robot data is also possible **CVE ID : CVE-2020-10264**	https://www.universal-robots.com/how-tos-and-faqs/how-to/ur-how-tos/real-time-data-exchange-rtde-guide/	H-UNI-UR3-270420/1010
Missing Authentication for Critical Function	06-04-2020	9	Universal Robots Robot Controllers Version CB2 SW Version 1.4 upwards, CB3 SW Version 3.0 and upwards, e-series SW Version 5.0 and upwards expose a service called DashBoard server at port 29999 that allows for control over core robot functions like starting/stopping programs, shutdown, reset safety and more. The DashBoard server is not protected by any kind of authentication or authorization.	https://www.universal-robots.com/how-tos-and-faqs/how-to/ur-how-tos/real-time-data-exchange-rtde-guide/	H-UNI-UR3-270420/1011

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-10265		
Insufficient Verification of Data Authenticity	06-04-2020	6.8	UR+ (Universal Robots+) is a platform of hardware and software component sellers, for Universal Robots robots. When installing any of these components in the robots (e.g. in the UR10), no integrity checks are performed. Moreover, the SDK for making such components can be easily obtained from Universal Robots. An attacker could exploit this flaw by crafting a custom component with the SDK, performing Person-In-The-Middle attacks (PITM) and shipping the maliciously-crafted component on demand. **CVE ID : CVE-2020-10266**	https://github.com/aliasrobotics/RVD/issues/1487	H-UNI-UR3-270420/1012
Missing Encryption of Sensitive Data	06-04-2020	5	Universal Robots control box CB 3.1 across firmware versions (tested on 1.12.1, 1.12, 1.11 and 1.10) does not encrypt or protect in any way the intellectual property artifacts installed from the UR+ platform of hardware and software components (URCaps). These files (*.urcaps) are stored under '/root/.urcaps' as plain	https://github.com/aliasrobotics/RVD/issues/1489	H-UNI-UR3-270420/1013

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			zip files containing all the logic to add functionality to the UR3, UR5 and UR10 robots. This flaw allows attackers with access to the robot or the robot network (while in combination with other flaws) to retrieve and easily exfiltrate all installed intellectual property. **CVE ID : CVE-2020-10267**		
ur5					
Information Exposure	06-04-2020	5.8	CB3 SW Version 3.3 and upwards, e-series SW Version 5.0 and upwards allow authenticated access to the RTDE (Real-Time Data Exchange) interface on port 30004 which allows setting registers, the speed slider fraction as well as digital and analog Outputs. Additionally unautheticated reading of robot data is also possible **CVE ID : CVE-2020-10264**	https://www.universal-robots.com/how-tos-and-faqs/how-to/ur-how-tos/real-time-data-exchange-rtde-guide/	H-UNI-UR5-270420/1014
Missing Authentication for Critical Function	06-04-2020	9	Universal Robots Robot Controllers Version CB2 SW Version 1.4 upwards, CB3 SW Version 3.0 and upwards, e-series SW Version 5.0 and upwards expose a service called DashBoard server at port 29999 that allows for	https://www.universal-robots.com/how-tos-and-faqs/how-to/ur-how-tos/real-	H-UNI-UR5-270420/1015

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			control over core robot functions like starting/stopping programs, shutdown, reset safety and more. The DashBoard server is not protected by any kind of authentication or authorization. **CVE ID : CVE-2020-10265**	time-data-exchange-rtde-guide/	
Insufficient Verification of Data Authenticity	06-04-2020	6.8	UR+ (Universal Robots+) is a platform of hardware and software component sellers, for Universal Robots robots. When installing any of these components in the robots (e.g. in the UR10), no integrity checks are performed. Moreover, the SDK for making such components can be easily obtained from Universal Robots. An attacker could exploit this flaw by crafting a custom component with the SDK, performing Person-In-The-Middle attacks (PITM) and shipping the maliciously-crafted component on demand. **CVE ID : CVE-2020-10266**	https://github.com/aliasrobotics/RVD/issues/1487	H-UNI-UR5-270420/1016
Missing Encryption of Sensitive Data	06-04-2020	5	Universal Robots control box CB 3.1 across firmware versions (tested on 1.12.1, 1.12, 1.11 and 1.10) does not encrypt or	https://github.com/aliasrobotics/RVD/issues/1489	H-UNI-UR5-270420/1017

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protect in any way the intellectual property artifacts installed from the UR+ platform of hardware and software components (URCaps). These files (*.urcaps) are stored under '/root/.urcaps' as plain zip files containing all the logic to add functionality to the UR3, UR5 and UR10 robots. This flaw allows attackers with access to the robot or the robot network (while in combination with other flaws) to retrieve and easily exfiltrate all installed intellectual property. **CVE ID : CVE-2020-10267**		
ur10e					
Information Exposure	06-04-2020	5.8	CB3 SW Version 3.3 and upwards, e-series SW Version 5.0 and upwards allow authenticated access to the RTDE (Real-Time Data Exchange) interface on port 30004 which allows setting registers, the speed slider fraction as well as digital and analog Outputs. Additionally unautheticated reading of robot data is also possible **CVE ID : CVE-2020-10264**	https://www.universal-robots.com/how-tos-and-faqs/how-to/ur-how-tos/real-time-data-exchange-rtde-guide/	H-UNI-UR10-270420/1018

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	06-04-2020	9	Universal Robots Robot Controllers Version CB2 SW Version 1.4 upwards, CB3 SW Version 3.0 and upwards, e-series SW Version 5.0 and upwards expose a service called DashBoard server at port 29999 that allows for control over core robot functions like starting/stopping programs, shutdown, reset safety and more. The DashBoard server is not protected by any kind of authentication or authorization. **CVE ID : CVE-2020-10265**	https://www.universal-robots.com/how-tos-and-faqs/how-to/ur-how-tos/real-time-data-exchange-rtde-guide/	H-UNI-UR10-270420/1019
ur3e					
Information Exposure	06-04-2020	5.8	CB3 SW Version 3.3 and upwards, e-series SW Version 5.0 and upwards allow authenticated access to the RTDE (Real-Time Data Exchange) interface on port 30004 which allows setting registers, the speed slider fraction as well as digital and analog Outputs. Additionally unautheticated reading of robot data is also possible **CVE ID : CVE-2020-10264**	https://www.universal-robots.com/how-tos-and-faqs/how-to/ur-how-tos/real-time-data-exchange-rtde-guide/	H-UNI-UR3E-270420/1020
Missing Authentication for Critical	06-04-2020	9	Universal Robots Robot Controllers Version CB2 SW Version 1.4 upwards,	https://www.universal-	H-UNI-UR3E-270420/1021

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Function			CB3 SW Version 3.0 and upwards, e-series SW Version 5.0 and upwards expose a service called DashBoard server at port 29999 that allows for control over core robot functions like starting/stopping programs, shutdown, reset safety and more. The DashBoard server is not protected by any kind of authentication or authorization. **CVE ID : CVE-2020-10265**	robots.com /how-tos-and-faqs/how-to/ur-how-tos/real-time-data-exchange-rtde-guide/	
ur5e					
Information Exposure	06-04-2020	5.8	CB3 SW Version 3.3 and upwards, e-series SW Version 5.0 and upwards allow authenticated access to the RTDE (Real-Time Data Exchange) interface on port 30004 which allows setting registers, the speed slider fraction as well as digital and analog Outputs. Additionally unautheticated reading of robot data is also possible **CVE ID : CVE-2020-10264**	https://www.universal-robots.com /how-tos-and-faqs/how-to/ur-how-tos/real-time-data-exchange-rtde-guide/	H-UNI-UR5E-270420/1022
Missing Authentication for Critical Function	06-04-2020	9	Universal Robots Robot Controllers Version CB2 SW Version 1.4 upwards, CB3 SW Version 3.0 and upwards, e-series SW Version 5.0 and upwards	https://www.universal-robots.com /how-tos-and-	H-UNI-UR5E-270420/1023

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			expose a service called DashBoard server at port 29999 that allows for control over core robot functions like starting/stopping programs, shutdown, reset safety and more. The DashBoard server is not protected by any kind of authentication or authorization. **CVE ID : CVE-2020-10265**	faqs/how-to/ur-how-tos/real-time-data-exchange-rtde-guide/	
Yamaha					
rtx830					
N/A	01-04-2020	7.8	Yamaha LTE VoIP Router(NVR700W firmware Rev.15.00.15 and earlier), Yamaha Gigabit VoIP Router(NVR510 firmware Rev.15.01.14 and earlier), Yamaha Gigabit VPN Router(RTX810 firmware Rev.11.01.33 and earlier, RTX830 firmware Rev.15.02.09 and earlier, RTX1200 firmware Rev.10.01.76 and earlier, RTX1210 firmware Rev.14.01.33 and earlier, RTX3500 firmware Rev.14.00.26 and earlier, and RTX5000 firmware Rev.14.00.26 and earlier), Yamaha Broadband VoIP Router(NVR500 firmware Rev.11.00.38 and earlier), and Yamaha	N/A	H-YAM-RTX8-270420/1024

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Firewall(FWX120 firmware Rev.11.03.27 and earlier) allow remote attackers to cause a denial of service via unspecified vectors. **CVE ID : CVE-2020-5548**		
nvr510					
N/A	01-04-2020	7.8	Yamaha LTE VoIP Router(NVR700W firmware Rev.15.00.15 and earlier), Yamaha Gigabit VoIP Router(NVR510 firmware Rev.15.01.14 and earlier), Yamaha Gigabit VPN Router(RTX810 firmware Rev.11.01.33 and earlier, RTX830 firmware Rev.15.02.09 and earlier, RTX1200 firmware Rev.10.01.76 and earlier, RTX1210 firmware Rev.14.01.33 and earlier, RTX3500 firmware Rev.14.00.26 and earlier, and RTX5000 firmware Rev.14.00.26 and earlier), Yamaha Broadband VoIP Router(NVR500 firmware Rev.11.00.38 and earlier), and Yamaha Firewall(FWX120 firmware Rev.11.03.27 and earlier) allow remote attackers to cause a denial of service via unspecified vectors. **CVE ID : CVE-2020-5548**	N/A	H-YAM-NVR5-270420/1025

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
nvr700w					
N/A	01-04-2020	7.8	Yamaha LTE VoIP Router(NVR700W firmware Rev.15.00.15 and earlier), Yamaha Gigabit VoIP Router(NVR510 firmware Rev.15.01.14 and earlier), Yamaha Gigabit VPN Router(RTX810 firmware Rev.11.01.33 and earlier, RTX830 firmware Rev.15.02.09 and earlier, RTX1200 firmware Rev.10.01.76 and earlier, RTX1210 firmware Rev.14.01.33 and earlier, RTX3500 firmware Rev.14.00.26 and earlier, and RTX5000 firmware Rev.14.00.26 and earlier), Yamaha Broadband VoIP Router(NVR500 firmware Rev.11.00.38 and earlier), and Yamaha Firewall(FWX120 firmware Rev.11.03.27 and earlier) allow remote attackers to cause a denial of service via unspecified vectors. **CVE ID : CVE-2020-5548**	N/A	H-YAM-NVR7-270420/1026
rtx1210					
N/A	01-04-2020	7.8	Yamaha LTE VoIP Router(NVR700W firmware Rev.15.00.15 and earlier), Yamaha Gigabit VoIP Router(NVR510 firmware Rev.15.01.14 and earlier),	N/A	H-YAM-RTX1-270420/1027

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Yamaha Gigabit VPN Router(RTX810 firmware Rev.11.01.33 and earlier, RTX830 firmware Rev.15.02.09 and earlier, RTX1200 firmware Rev.10.01.76 and earlier, RTX1210 firmware Rev.14.01.33 and earlier, RTX3500 firmware Rev.14.00.26 and earlier, and RTX5000 firmware Rev.14.00.26 and earlier), Yamaha Broadband VoIP Router(NVR500 firmware Rev.11.00.38 and earlier), and Yamaha Firewall(FWX120 firmware Rev.11.03.27 and earlier) allow remote attackers to cause a denial of service via unspecified vectors. **CVE ID : CVE-2020-5548**		
rtx5000					
N/A	01-04-2020	7.8	Yamaha LTE VoIP Router(NVR700W firmware Rev.15.00.15 and earlier), Yamaha Gigabit VoIP Router(NVR510 firmware Rev.15.01.14 and earlier), Yamaha Gigabit VPN Router(RTX810 firmware Rev.11.01.33 and earlier, RTX830 firmware Rev.15.02.09 and earlier, RTX1200 firmware Rev.10.01.76 and earlier, RTX1210 firmware	N/A	H-YAM-RTX5-270420/1028

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rev.14.01.33 and earlier, RTX3500 firmware Rev.14.00.26 and earlier, and RTX5000 firmware Rev.14.00.26 and earlier), Yamaha Broadband VoIP Router(NVR500 firmware Rev.11.00.38 and earlier), and Yamaha Firewall(FWX120 firmware Rev.11.03.27 and earlier) allow remote attackers to cause a denial of service via unspecified vectors. **CVE ID : CVE-2020-5548**		
rtx3500					
N/A	01-04-2020	7.8	Yamaha LTE VoIP Router(NVR700W firmware Rev.15.00.15 and earlier), Yamaha Gigabit VoIP Router(NVR510 firmware Rev.15.01.14 and earlier), Yamaha Gigabit VPN Router(RTX810 firmware Rev.11.01.33 and earlier, RTX830 firmware Rev.15.02.09 and earlier, RTX1200 firmware Rev.10.01.76 and earlier, RTX1210 firmware Rev.14.01.33 and earlier, RTX3500 firmware Rev.14.00.26 and earlier, and RTX5000 firmware Rev.14.00.26 and earlier), Yamaha Broadband VoIP Router(NVR500 firmware Rev.11.00.38 and earlier),	N/A	H-YAM-RTX3-270420/1029

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and Yamaha Firewall(FWX120 firmware Rev.11.03.27 and earlier) allow remote attackers to cause a denial of service via unspecified vectors. **CVE ID : CVE-2020-5548**		
nvr500					
N/A	01-04-2020	7.8	Yamaha LTE VoIP Router(NVR700W firmware Rev.15.00.15 and earlier), Yamaha Gigabit VoIP Router(NVR510 firmware Rev.15.01.14 and earlier), Yamaha Gigabit VPN Router(RTX810 firmware Rev.11.01.33 and earlier, RTX830 firmware Rev.15.02.09 and earlier, RTX1200 firmware Rev.10.01.76 and earlier, RTX1210 firmware Rev.14.01.33 and earlier, RTX3500 firmware Rev.14.00.26 and earlier, and RTX5000 firmware Rev.14.00.26 and earlier), Yamaha Broadband VoIP Router(NVR500 firmware Rev.11.00.38 and earlier), and Yamaha Firewall(FWX120 firmware Rev.11.03.27 and earlier) allow remote attackers to cause a denial of service via unspecified vectors. **CVE ID : CVE-2020-5548**	N/A	H-YAM-NVR5-270420/1030

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Rtx1200					
N/A	01-04-2020	7.8	Yamaha LTE VoIP Router(NVR700W firmware Rev.15.00.15 and earlier), Yamaha Gigabit VoIP Router(NVR510 firmware Rev.15.01.14 and earlier), Yamaha Gigabit VPN Router(RTX810 firmware Rev.11.01.33 and earlier, RTX830 firmware Rev.15.02.09 and earlier, RTX1200 firmware Rev.10.01.76 and earlier, RTX1210 firmware Rev.14.01.33 and earlier, RTX3500 firmware Rev.14.00.26 and earlier, and RTX5000 firmware Rev.14.00.26 and earlier), Yamaha Broadband VoIP Router(NVR500 firmware Rev.11.00.38 and earlier), and Yamaha Firewall(FWX120 firmware Rev.11.03.27 and earlier) allow remote attackers to cause a denial of service via unspecified vectors. **CVE ID : CVE-2020-5548**	N/A	H-YAM-RTX1-270420/1031
Fwx120					
N/A	01-04-2020	7.8	Yamaha LTE VoIP Router(NVR700W firmware Rev.15.00.15 and earlier), Yamaha Gigabit VoIP Router(NVR510 firmware Rev.15.01.14 and earlier),	N/A	H-YAM-FWX1-270420/1032

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Yamaha Gigabit VPN Router(RTX810 firmware Rev.11.01.33 and earlier, RTX830 firmware Rev.15.02.09 and earlier, RTX1200 firmware Rev.10.01.76 and earlier, RTX1210 firmware Rev.14.01.33 and earlier, RTX3500 firmware Rev.14.00.26 and earlier, and RTX5000 firmware Rev.14.00.26 and earlier), Yamaha Broadband VoIP Router(NVR500 firmware Rev.11.00.38 and earlier), and Yamaha Firewall(FWX120 firmware Rev.11.03.27 and earlier) allow remote attackers to cause a denial of service via unspecified vectors. **CVE ID : CVE-2020-5548**		
Rtx810					
N/A	01-04-2020	7.8	Yamaha LTE VoIP Router(NVR700W firmware Rev.15.00.15 and earlier), Yamaha Gigabit VoIP Router(NVR510 firmware Rev.15.01.14 and earlier), Yamaha Gigabit VPN Router(RTX810 firmware Rev.11.01.33 and earlier, RTX830 firmware Rev.15.02.09 and earlier, RTX1200 firmware Rev.10.01.76 and earlier, RTX1210 firmware	N/A	H-YAM-RTX8-270420/1033

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rev.14.01.33 and earlier, RTX3500 firmware Rev.14.00.26 and earlier, and RTX5000 firmware Rev.14.00.26 and earlier), Yamaha Broadband VoIP Router(NVR500 firmware Rev.11.00.38 and earlier), and Yamaha Firewall(FWX120 firmware Rev.11.03.27 and earlier) allow remote attackers to cause a denial of service via unspecified vectors. **CVE ID : CVE-2020-5548**		