



<https://nciipc.gov.in>

National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures(CVE) Report

16 - 30 Apr 2021

Vol. 08 No. 08

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Application										
acemetrix										
jquery-deparam										
N/A	23-04-2021	6.5	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in jquery-deparam 0.5.1 allows a malicious user to inject properties into Object.prototype. CVE ID : CVE-2021-20087	N/A	A-ACE-JQUE-040521/1					
adobe										
robohelp										
Uncontrolled Search Path Element	19-04-2021	9.3	Adobe Robohelp version 2020.0.3 (and earlier) is affected by an uncontrolled search path element vulnerability that could lead to privilege escalation. An attacker with permissions to write to the file system could leverage this vulnerability to escalate privileges. CVE ID : CVE-2021-21070	https://helpx.adobe.com/security/products/robohelp/apsb21-20.html	A-ADO-ROBO-040521/2					
adtran										
personal_phone_manager										
Improper Neutralization of Input During Web Page Generation ('Cross-site	20-04-2021	3.5	** UNSUPPORTED WHEN ASSIGNED ** The AdTran Personal Phone Manager software is vulnerable to an authenticated stored cross-site scripting (XSS) issues. These issues impact at minimum versions 10.8.1	http://adtran.com	A-ADT-PERS-040521/3					
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
Scripting')			and below but potentially impact later versions as well since they have not previously been disclosed. Only version 10.8.1 was able to be confirmed during primary research. NOTE: The affected appliances NetVanta 7060 and NetVanta 7100 are considered End of Life and as such this issue will not be patched. CVE ID : CVE-2021-25679		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-04-2021	4.3	** UNSUPPORTED WHEN ASSIGNED ** The AdTran Personal Phone Manager software is vulnerable to multiple reflected cross-site scripting (XSS) issues. These issues impact at minimum versions 10.8.1 and below but potentially impact later versions as well since they have not previously been disclosed. Only version 10.8.1 was able to be confirmed during primary research. NOTE: The affected appliances NetVanta 7060 and NetVanta 7100 are considered End of Life and as such this issue will not be patched. CVE ID : CVE-2021-25680	http://adtran.com	A-ADT-PERS-040521/4
N/A	20-04-2021	5	** UNSUPPORTED WHEN ASSIGNED ** AdTran Personal Phone Manager 10.8.1 software is vulnerable to an issue that allows for exfiltration of data over DNS. This could	http://adtran.com	A-ADT-PERS-040521/5

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow for exposed AdTran Personal Phone Manager web servers to be used as DNS redirectors to tunnel arbitrary data over DNS. NOTE: The affected appliances NetVanta 7060 and NetVanta 7100 are considered End of Life and as such this issue will not be patched. CVE ID : CVE-2021-25681		
advancedcustomfields					
advanced_custom_fields					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2021	4.3	The Advanced Custom Fields Pro WordPress plugin before 5.9.1 did not properly escape the generated update URL when outputting it in an attribute, leading to a reflected Cross-Site Scripting issue in the update settings page. CVE ID : CVE-2021-24241	https://wpscan.com/vulnerability/d1e9c995-37bd-4952-b88e-945e02e3c83f , https://www.advancedcustomfields.com/blog/acf-5-9-1-release/	A-ADV-ADVA-040521/6
aivahthemes					
business_hours_pro					
Unrestricted Upload of File with Dangerous Type	22-04-2021	7.5	The Business Hours Pro WordPress plugin through 5.5.0 allows a remote attacker to upload arbitrary files using its manual update functionality, leading to an unauthenticated remote code execution vulnerability. CVE ID : CVE-2021-24240	https://wpscan.com/vulnerability/10528cb2-12a1-43f7-9b7d-d75d18fdf5bb	A-AIV-BUSI-040521/7

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
atlassian					
connect_express					
Incorrect Authorization	16-04-2021	4	<p>Broken Authentication in Atlassian Connect Express (ACE) from version 3.0.2 before version 6.6.0: Atlassian Connect Express is a Node.js package for building Atlassian Connect apps. Authentication between Atlassian products and the Atlassian Connect Express app occurs with a server-to-server JWT or a context JWT. Atlassian Connect Express versions between 3.0.2 - 6.5.0 erroneously accept context JWTs in lifecycle endpoints (such as installation) where only server-to-server JWTs should be accepted, permitting an attacker to send authenticated re-installation events to an app.</p> <p>CVE ID : CVE-2021-26073</p>	<p>https://confluence.atlassian.com/pages/viewpage.action?pageId=1051986099, https://community.developer.atlassian.com/t/action-required-atlassian-connect-vulnerability-a[...]ypass-of-app-qsh-verification-via-context-jwts/47072</p>	A-ATL-CONN-040521/8
connect_spring_boot					
Incorrect Authorization	16-04-2021	4	<p>Broken Authentication in Atlassian Connect Spring Boot (ACSB) from version 1.1.0 before version 2.1.3: Atlassian Connect Spring Boot is a Java Spring Boot package for building Atlassian Connect apps. Authentication between Atlassian products and the Atlassian Connect Spring Boot app occurs with a server-to-server JWT or a context JWT. Atlassian</p>	<p>https://confluence.atlassian.com/pages/viewpage.action?pageId=1051986106, https://community.developer.atlassian.com/t/action-required-atlassian-connect-</p>	A-ATL-CONN-040521/9

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connect Spring Boot versions between 1.1.0 - 2.1.2 erroneously accept context JWTs in lifecycle endpoints (such as installation) where only server-to-server JWTs should be accepted, permitting an attacker to send authenticated re-installation events to an app. CVE ID : CVE-2021-26074	vulnerability -allows-bypass-of-app-qsh-verification-via-context-jwts/47072	

authelia

authelia

URL Redirection to Untrusted Site ('Open Redirect')	21-04-2021	4.9	Authelia is an open-source authentication and authorization server providing 2-factor authentication and single sign-on (SSO) for your applications via a web portal. In versions 4.27.4 and earlier, utilizing a HTTP query parameter an attacker is able to redirect users from the web application to any domain, including potentially malicious sites. This security issue does not directly impact the security of the web application itself. As a workaround, one can use a reverse proxy to strip the query parameter from the affected endpoint. There is a patch for version 4.28.0. CVE ID : CVE-2021-29456	https://github.com/authelia/authelia/security/advisories/GHSA-36f2-fcrx-fp4j	A-AUT-AUTH-040521/10
---	------------	-----	---	---	----------------------

autodesk

fbx_review

CVSS Scoring Scale	0-1	1-2	2-3	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	19-04-2021	6.8	A Memory Corruption Vulnerability in Autodesk FBX Review version 1.4.0 may lead to remote code execution through maliciously crafted DLL files. CVE ID : CVE-2021-27028	https://www.autodesk.com/trust/security-advisories/a-dsk-sa-2021-0001	A-AUT-FBX_-040521/11
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-04-2021	9.3	A user may be tricked into opening a malicious FBX file which may exploit a Directory Traversal Remote Code Execution vulnerability in FBX's Review causing it to run arbitrary code on the system. CVE ID : CVE-2021-27030	https://www.autodesk.com/trust/security-advisories/a-dsk-sa-2021-0001	A-AUT-FBX_-040521/12
Use After Free	19-04-2021	9.3	A user may be tricked into opening a malicious FBX file which may exploit a use-after-free vulnerability in FBX's Review causing the application to reference a memory location controlled by an unauthorized third party, thereby running arbitrary code on the system. CVE ID : CVE-2021-27031	https://www.autodesk.com/trust/security-advisories/a-dsk-sa-2021-0001	A-AUT-FBX_-040521/13
Out-of-bounds Write	19-04-2021	6.8	A Out-Of-Bounds Read/Write Vulnerability in Autodesk FBX Review version 1.4.0 may lead to remote code execution through maliciously crafted DLL files or information disclosure. CVE ID : CVE-2021-27027	https://www.autodesk.com/trust/security-advisories/a-dsk-sa-2021-0001	A-AUT-FBX_-040521/14
NULL Pointer Dereference	19-04-2021	4.3	The user may be tricked into opening a malicious	https://www.autodesk.com/trust/security-advisories/a-dsk-sa-2021-0001	A-AUT-FBX_-040521/15

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			FBX file which may exploit a Null Pointer Dereference vulnerability in FBX's Review causing the application to crash leading to a denial of service. CVE ID : CVE-2021-27029	om/trust/security-advisories/a-dsk-sa-2021-0001						
backbone-query-parameters_project										
backbone-query-parameters										
N/A	23-04-2021	6.5	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in backbone-query-parameters 0.4.0 allows a malicious user to inject properties into Object.prototype. CVE ID : CVE-2021-20085	N/A	A-BAC-BACK-040521/16					
boostifythemes										
goto										
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2021	4.3	The Goto WordPress theme before 2.0 does not sanitise the keywords and start_date GET parameter on its Tour List page, leading to an unauthenticated reflected Cross-Site Scripting issue. CVE ID : CVE-2021-24235	https://wpscan.com/vulnerability/ece90aa-582b-4c49-8b7c-14027f9df139	A-BOO-GOTO-040521/17					
boxystudio										
cooked										
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2021	4.3	The Cooked Pro WordPress plugin before 1.7.5.6 was affected by unauthenticated reflected Cross-Site Scripting issues, due to improper sanitisation of user input while being output back in pages as an	https://wpscan.com/vulnerability/d620de5-1ad2-4480-b08b-719480472bc0	A-BOX-COOK-040521/18					
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
			arbitrary attribute. CVE ID : CVE-2021-24233		
checkpoint					
identity_agent					
N/A	22-04-2021	5.5	A denial of service vulnerability was reported in Check Point Identity Agent before R81.018.0000, which could allow low privileged users to overwrite protected system files. CVE ID : CVE-2021-30356	https://supportcontent.checkpoint.com/solutions?id=sk134312	A-CHE-IDEN-040521/19
criticalmanufacturing					
cncsoft-b					
Out-of-bounds Write	27-04-2021	6.8	CNCSoft-B Versions 1.0.0.3 and prior is vulnerable to an out-of-bounds write, which may allow an attacker to execute arbitrary code. CVE ID : CVE-2021-22664	N/A	A-CRI-CNCS-040521/20
curveballjs					
a12n-server					
Improper Privilege Management	16-04-2021	4	a12n-server is an npm package which aims to provide a simple authentication system. A new HAL-Form was added to allow editing users in version 0.18.0. This feature should only have been accessible to admins. Unfortunately, privileges were incorrectly checked allowing any logged in user to make this change. Patched in v0.18.2. CVE ID : CVE-2021-29452	https://github.com/curveball/a12n-server/security/advisories/GHSA-8hw9-22v6-9jr9	A-CUR-A12N-040521/21

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
dart					
dart_software_development_kit					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2021	4.3	Bad validation logic in the Dart SDK versions prior to 2.12.3 allow an attacker to use an XSS attack via DOM clobbering. The validation logic in dart.html for creating DOM nodes from text did not sanitize properly when it came across template tags. CVE ID : CVE-2021-22540	https://github.com/dart-lang/sdk/security/advisories/GHSA-3rfv-4jvg-9522 , https://github.com/dart-lang/sdk/commit/ce5a1c2392debce967415d4c09359ff255e3588	A-DAR-DART-040521/22
dell					
powerscale_onefs					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-04-2021	7.2	Dell PowerScale OneFS 8.1.0 - 9.1.0 contains a privilege escalation in SmartLock compliance mode that may allow compadmin to execute arbitrary commands as root. CVE ID : CVE-2021-21526	https://www.dell.com/support/kbdoc/000185202	A-DEL-POWE-040521/23
directum					
directum					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-04-2021	4.3	Settings.aspx?view=About in Directum 5.8.2 allows XSS via the HTTP User-Agent header. CVE ID : CVE-2021-31794	https://www.directum.ru/	A-DIR-DIRE-040521/24

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
discord					
discord-recon					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-04-2021	5	Discord-Recon is a bot for the Discord chat service. In versions of Discord-Recon 0.0.3 and prior, a remote attacker is able to read local files from the server that can disclose important information. As a workaround, a bot maintainer can locate the file `app.py` and add `replace('..', '')` into the `Path` variable inside of the `recon` function. The vulnerability is patched in version 0.0.4. CVE ID : CVE-2021-29466	https://github.com/DEMON1A/Discord-Recon/security/advisories/GHSA-p2pw-8xwf-879g	A-DIS-DISC-040521/25
Improper Control of Generation of Code ('Code Injection')	22-04-2021	7.5	Discord-Recon is a bot for the Discord chat service. Versions of Discord-Recon 0.0.3 and prior contain a vulnerability in which a remote attacker is able to overwrite any file on the system with the command results. This can result in remote code execution when the user overwrite important files on the system. As a workaround, bot maintainers can edit their `setting.py` file then add `<` and `>` into the `RCE` variable inside of it to fix the issue without an update. The vulnerability is patched in version 0.0.4. CVE ID : CVE-2021-29465	https://github.com/DEMON1A/Discord-Recon/security/advisories/GHSA-6pp2-rpj3-jcix	A-DIS-DISC-040521/26
discord-recon_project					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
discord-recon					
Improper Control of Generation of Code ('Code Injection')	20-04-2021	9	<p>### Impact - This issue could be exploited to read internal files from the system and write files into the system resulting in remote code execution ###</p> <p>Patches - This issue has been fixed on 0.0.3 version by adding a regex that validate if there's any arguments on the command. then disallow execution if there's an argument ###</p> <p>Workarounds - To fix this issue from your side, just upgrade discord-recon, if you're unable to do that. then just copy the code from `assets/CommandInjection.py` and overwrite your code with the new one. that's the only code required. ###</p> <p>Credits - All of the credits for finding these issues on discord-recon goes to Omar Badran. ### For more information If you have any questions or comments about this advisory: * Email us at mdaif1332@gmail.com</p> <p>CVE ID : CVE-2021-29461</p>	https://github.com/DEMON1A/Discord-Recon/security/advisories/GHSA-3m9v-v33c-g83x	A-DIS-DISC-040521/27
eclipse					
jersey					
Incorrect Permission Assignment	22-04-2021	2.1	Eclipse Jersey 2.28 to 2.33 and Eclipse Jersey 3.0.0 to 3.0.1 contains a local	https://github.com/eclipse-	A-ECL-JERS-040521/28

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
for Critical Resource			information disclosure vulnerability. This is due to the use of the File.createTempFile which creates a file inside of the system temporary directory with the permissions: -rw-r--r--. Thus the contents of this file are viewable by all other users locally on the system. As such, if the contents written is security sensitive, it can be disclosed to other local users. CVE ID : CVE-2021-28168	ee4j/jersey/security/adv isories/GHS A-c43q- 5hpj-4crv, https://github.com/eclipse-ee4j/jersey/pull/4712	
openj9					
Missing Initialization of Resource	21-04-2021	6.4	In Eclipse Openj9 to version 0.25.0, usage of the jdk.internal.reflect.Constant Pool API causes the JVM in some cases to pre-resolve certain constant pool entries. This allows a user to call static methods or access static members without running the class initialization method, and may allow a user to observe uninitialized values. CVE ID : CVE-2021-28167	https://github.com/eclipse/openj9/issues/12016	A-ECL-OPEN-040521/29
elbtide					
advanced_booking_calendar					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2021	3.5	The Advanced Booking Calendar WordPress plugin before 1.6.8 does not sanitise the license error message when output in the settings page, leading to an authenticated reflected Cross-Site Scripting issue CVE ID : CVE-2021-24232	https://wpscan.com/vulnerability/f06629b5-8b15-48eb-a7a7-78b693e06b71	A-ELB-ADVA-040521/30

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						
exiv2											
exiv2											
Out-of-bounds Read	19-04-2021	4.3	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. An out-of-bounds read was found in Exiv2 versions v0.27.3 and earlier. The out-of-bounds read is triggered when Exiv2 is used to write metadata into a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service by crashing Exiv2, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when writing the metadata, which is a less frequently used Exiv2 operation than reading the metadata. For example, to trigger the bug in the Exiv2 command-line application, you need to add an extra command-line argument such as insert. The bug is fixed in version v0.27.4. CVE ID : CVE-2021-29458	https://github.com/Exiv2/exiv2/pull/1536 , https://github.com/Exiv2/exiv2/security/advisories/GHSA-57jj-75fm-9rq5	A-EXI-EXIV-040521/31						
Heap-based Buffer Overflow	19-04-2021	6.8	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. A heap buffer overflow was found in Exiv2 versions v0.27.3 and earlier. The heap overflow is triggered when Exiv2 is used to write metadata into	https://github.com/Exiv2/exiv2/issues/1529 , https://github.com/Exiv2/exiv2/pull/1534 , https://github.com/Exiv2/exiv2/pull/1534	A-EXI-EXIV-040521/32						
CVSS Scoring Scale		0-1	1-2	2-3	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 crafted image file. An attacker could potentially exploit the vulnerability to gain code execution, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when <code>_writing_</code> the metadata, which is a less frequently used Exiv2 operation than <code>_reading_</code> the metadata. For example, to trigger the bug in the Exiv2 command-line application, you need to add an extra command-line argument such as <code>'insert'</code> . The bug is fixed in version v0.27.4. CVE ID : CVE-2021-29457	2/exiv2/security/advisories/GHSA-v74w-h496-cgqm	

ezxml_project

ezxml

XML Injection (aka Blind XPath Injection)	16-04-2021	4.3	An issue was discovered in libezxml.a in ezXML 0.8.6. The function <code>ezxml_parse_str()</code> performs incorrect memory handling while parsing crafted XML files (writing outside a memory region created by <code>mmap</code>). CVE ID : CVE-2021-31347	https://sourceforge.net/p/ezxml/bugs/27/	A-EZX-EZXM-040521/33
XML Injection (aka Blind XPath Injection)	16-04-2021	4.3	An issue was discovered in libezxml.a in ezXML 0.8.6. The function <code>ezxml_parse_str()</code> performs incorrect memory handling while parsing crafted XML files (out-of-bounds read after a certain <code>strcspn</code> failure).	https://sourceforge.net/p/ezxml/bugs/27/	A-EZX-EZXM-040521/34

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
			CVE ID : CVE-2021-31348		
ffmpegdotjs_project					
ffmpegdotjs					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-04-2021	7.5	This affects all versions of package ffmpegdotjs. If attacker-controlled user input is given to the trimvideo function, it is possible for an attacker to execute arbitrary commands. This is due to use of the child_process exec function without input sanitization. CVE ID : CVE-2021-23376	N/A	A-FFM-FFMP-040521/35
fusionauth					
saml_v2					
Improper Restriction of XML External Entity Reference	22-04-2021	4	FusionAuth fusionauth-samlv2 before 0.5.4 allows XXE attacks via a forged AuthnRequest or LogoutRequest because parseFromBytes uses javax.xml.parsers.DocumentBuilderFactory unsafely. CVE ID : CVE-2021-27736	https://github.com/FusionAuth/fusionauth-samlv2/compare/0.5.3...0.5.4 , https://github.com/FusionAuth/fusionauth-samlv2/commit/c66fb689d50010662f705d5b585c6388ce555dbd	A-FUS-SAML-040521/36
genetechsolutions					
pie_register					
Improper Neutralization of Input During Web	22-04-2021	4.3	The Pie Register “ User Registration Forms. Invitation based registrations, Custom Login,	https://wpscan.com/vulnerability/f1b67f40-	A-GEN-PIE_-040521/37

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Page Generation ('Cross-site Scripting')			Payments WordPress plugin before 3.7.0.1 does not sanitise the invitaion_code GET parameter when outputting it in the Activation Code page, leading to a reflected Cross-Site Scripting issue. CVE ID : CVE-2021-24239	642f-451e-a67a-b7487918ee34, https://plugins.trac.wordpress.org/changeset/2507536/						
gitlab										
gitlab										
Improper Input Validation	23-04-2021	6.5	An issue has been discovered in GitLab CE/EE affecting all versions starting from 11.9. GitLab was not properly validating image files that were passed to a file parser which resulted in a remote command execution. CVE ID : CVE-2021-22205	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22205.json	A-GIT-GITL-040521/38					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2021	3.5	An issue has been discovered in GitLab affecting all versions starting with 12.9. GitLab was vulnerable to a stored XSS if scoped labels were used. CVE ID : CVE-2021-22199	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22199.json	A-GIT-GITL-040521/39					
google										
bazel										
Exposure of Resource to Wrong Sphere	16-04-2021	6.8	An attacker can place a crafted JSON config file into the project folder pointing to a custom executable. VScode-bazel allows the workspace path to lint *.bzl files to be set via this config file. As such the attacker is able to execute any executable on the system	N/A	A-GOO-BAZE-040521/40					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			through vscode-bazel. We recommend upgrading to version 0.4.1 or above. CVE ID : CVE-2021-22539		
chrome					
N/A	26-04-2021	5.8	Insufficient policy enforcement in navigation in Google Chrome on iOS prior to 90.0.4430.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. CVE ID : CVE-2021-21205	N/A	A-GOO-CHRO-040521/41
Use After Free	26-04-2021	6.8	Use after free in Blink in Google Chrome prior to 89.0.4389.128 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-21206	N/A	A-GOO-CHRO-040521/42
Use After Free	26-04-2021	6.8	Use after free in IndexedDB in Google Chrome prior to 90.0.4430.72 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension. CVE ID : CVE-2021-21207	N/A	A-GOO-CHRO-040521/43
Improper Input Validation	26-04-2021	4.3	Insufficient data validation in QR scanner in Google Chrome on iOS prior to 90.0.4430.72 allowed an attacker displaying a QR code to perform domain spoofing via a crafted QR code.	N/A	A-GOO-CHRO-040521/44

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-21208		
Improper Input Validation	26-04-2021	4.3	Insufficient validation of untrusted input in Mojo in Google Chrome prior to 90.0.4430.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. CVE ID : CVE-2021-21221	N/A	A-GOO-CHRO-040521/45
Out-of-bounds Write	26-04-2021	4.3	Heap buffer overflow in V8 in Google Chrome prior to 90.0.4430.85 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. CVE ID : CVE-2021-21222	N/A	A-GOO-CHRO-040521/46
Integer Overflow or Wraparound	26-04-2021	6.8	Integer overflow in Mojo in Google Chrome prior to 90.0.4430.85 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2021-21223	N/A	A-GOO-CHRO-040521/47
Access of Resource Using Incompatible Type ('Type Confusion')	26-04-2021	6.8	Type confusion in V8 in Google Chrome prior to 90.0.4430.85 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. CVE ID : CVE-2021-21224	N/A	A-GOO-CHRO-040521/48
Improper Restriction of Operations within the	26-04-2021	6.8	Out of bounds memory access in V8 in Google Chrome prior to 90.0.4430.85 allowed a	N/A	A-GOO-CHRO-040521/49

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-21225		
Use After Free	26-04-2021	6.8	Use after free in extensions in Google Chrome prior to 90.0.4430.72 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension. CVE ID : CVE-2021-21202	N/A	A-GOO-CHRO-040521/50
Use After Free	26-04-2021	6.8	Use after free in Blink in Google Chrome on OS X prior to 90.0.4430.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-21204	N/A	A-GOO-CHRO-040521/51
Origin Validation Error	26-04-2021	4.3	Inappropriate implementation in storage in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. CVE ID : CVE-2021-21209	N/A	A-GOO-CHRO-040521/52
Origin Validation Error	26-04-2021	4.3	Inappropriate implementation in Navigation in Google Chrome on iOS prior to 90.0.4430.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. CVE ID : CVE-2021-21211	N/A	A-GOO-CHRO-040521/53

CVSS Scoring Scale	0-1	1-2	2-3	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 of Uninitialized Resource	26-04-2021	4.3	Uninitialized data in PDFium in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted PDF file. CVE ID : CVE-2021-21218	N/A	A-GOO-CHRO-040521/54						
Improper Restriction of Operations within the Bounds of a Memory Buffer	26-04-2021	6.8	Insufficient validation of untrusted input in V8 in Google Chrome prior to 89.0.4389.128 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-21220	N/A	A-GOO-CHRO-040521/55						
Out-of-bounds Write	30-04-2021	6.8	Insufficient data validation in V8 in Google Chrome prior to 90.0.4430.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-21227	https://crbug.com/1199345 , https://chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop_26.html	A-GOO-CHRO-040521/56						
Use After Free	26-04-2021	6.8	Use after free in WebMIDI in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-21213	N/A	A-GOO-CHRO-040521/57						
Use After Free	26-04-2021	6.8	Use after free in Network API in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to	N/A	A-GOO-CHRO-040521/58						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially exploit heap corruption via a crafted Chrome Extension. CVE ID : CVE-2021-21214		
Authentication Bypass by Spoofing	26-04-2021	4.3	Inappropriate implementation in Autofill in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to spoof security UI via a crafted HTML page. CVE ID : CVE-2021-21215	https://chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop_14.html , https://crbug.com/1172533	A-GOO-CHRO-040521/59
Authentication Bypass by Spoofing	26-04-2021	4.3	Inappropriate implementation in Autofill in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to spoof security UI via a crafted HTML page. CVE ID : CVE-2021-21216	https://crbug.com/1173297 , https://chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop_14.html	A-GOO-CHRO-040521/60
Access of Resource Using Incompatible Type ('Type Confusion')	30-04-2021	6.8	Type confusion in V8 in Google Chrome prior to 90.0.4430.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-21230	https://chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop_26.html , https://crbug.com/1198705	A-GOO-CHRO-040521/61
Use After Free	30-04-2021	6.8	Use after free in Dev Tools in Google Chrome prior to	https://crbug.com/1175	A-GOO-CHRO-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			90.0.4430.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-21232	058, https://chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop_26.html	040521/62
Out-of-bounds Write	30-04-2021	6.8	Heap buffer overflow in ANGLE in Google Chrome on Windows prior to 90.0.4430.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-21233	https://crbug.com/1182937 , https://chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop_26.html	A-GOO-CHRO-040521/63
Use After Free	26-04-2021	6.8	Use after free in permissions in Google Chrome prior to 90.0.4430.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2021-21201	N/A	A-GOO-CHRO-040521/64
Use After Free	26-04-2021	6.8	Use after free in Blink in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-21203	N/A	A-GOO-CHRO-040521/65
Exposure of Resource to	26-04-2021	4.3	Inappropriate implementation in Network	N/A	A-GOO-CHRO-

CVSS Scoring Scale	0-1	1-2	2-3	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			in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to potentially access local UDP ports via a crafted HTML page. CVE ID : CVE-2021-21210		040521/66						
N/A	26-04-2021	4.3	Incorrect security UI in Network Config UI in Google Chrome on ChromeOS prior to 90.0.4430.72 allowed a remote attacker to potentially compromise WiFi connection security via a malicious WAP. CVE ID : CVE-2021-21212	N/A	A-GOO-CHRO-040521/67						
Exposure of Sensitive Information to an Unauthorized Actor	26-04-2021	4.3	Uninitialized data in PDFium in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted PDF file. CVE ID : CVE-2021-21217	https://crbug.com/1166462 , https://chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop_14.html	A-GOO-CHRO-040521/68						
Exposure of Sensitive Information to an Unauthorized Actor	26-04-2021	4.3	Uninitialized data in PDFium in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted PDF file. CVE ID : CVE-2021-21219	N/A	A-GOO-CHRO-040521/69						
Use After Free	26-04-2021	6.8	Use after free in navigation in Google Chrome prior to 90.0.4430.85 allowed a remote attacker who had compromised the renderer	N/A	A-GOO-CHRO-040521/70						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			process to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2021-21226		
gpac					
gpac					
NULL Pointer Dereference	19-04-2021	4.3	The HintFile function in GPAC 1.0.1 allows attackers to cause a denial of service (NULL pointer dereference) via a crafted file in the MP4Box command. CVE ID : CVE-2021-31257	https://github.com/gpac/gpac/commit/87afe070cd6866df7fe80f11b26ef75161de85e0	A-GPA-GPAC-040521/71
NULL Pointer Dereference	19-04-2021	4.3	The gf_isom_set_extraction_slc function in GPAC 1.0.1 allows attackers to cause a denial of service (NULL pointer dereference) via a crafted file in the MP4Box command. CVE ID : CVE-2021-31258	https://github.com/gpac/gpac/commit/ebfa346ef05049718f7b80041093b4c5581c24e	A-GPA-GPAC-040521/72
NULL Pointer Dereference	19-04-2021	4.3	The gf_isom_cenc_get_default_info_internal function in GPAC 1.0.1 allows attackers to cause a denial of service (NULL pointer dereference) via a crafted file in the MP4Box command. CVE ID : CVE-2021-31259	https://github.com/gpac/gpac/commit/3b84ffcba9cf144ce35650df958432f472b6483f8	A-GPA-GPAC-040521/73
NULL Pointer Dereference	19-04-2021	4.3	The MergeTrack function in GPAC 1.0.1 allows attackers to cause a denial of service (NULL pointer dereference) via a crafted file in the MP4Box command. CVE ID : CVE-2021-31260	https://github.com/gpac/gpac/commit/df8fffd839fe5ae9acd82d26fd48280a397411d9	A-GPA-GPAC-040521/74
Improper Restriction of	19-04-2021	4.3	Memory leak in the stbl_GetSampleInfos	https://github.com/gpac/gpac	A-GPA-GPAC-

CVSS Scoring Scale	0-1	1-2	2-3	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			function in MP4Box in GPAC 1.0.1 allows attackers to read memory via a crafted file. CVE ID : CVE-2021-31256	/gpac/comm it/2da2f68bf fd51d89b1d 272d22aa8c c023c1c066 e	040521/75
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-04-2021	4.3	The gf_hinter_track_new function in GPAC 1.0.1 allows attackers to read memory via a crafted file in the MP4Box command. CVE ID : CVE-2021-31261	https://github.com/gpac/gpac/commit/cd3738dea038dbd12e603ad48cd7373ae0440f65	A-GPA-GPAC-040521/76
Out-of-bounds Write	19-04-2021	6.8	There is a integer overflow in function filter_core/filter_props.c:gf_props_assign_value in GPAC 1.0.1. In which, the arg const GF_PropertyValue *value,maybe value->value.data.size is a negative number. In result, memcpy in gf_props_assign_value failed. CVE ID : CVE-2021-29279	https://github.com/gpac/gpac/commit/da69ad1f970a7e17c865eaec9af98cc84df10d5b	A-GPA-GPAC-040521/77
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-04-2021	6.8	Buffer overflow in the abst_box_read function in MP4Box in GPAC 1.0.1 allows attackers to cause a denial of service or execute arbitrary code via a crafted file. CVE ID : CVE-2021-31255	https://github.com/gpac/gpac/commit/758135e91e623d7dfe7f6aaad7aeb3f791b7a4e5	A-GPA-GPAC-040521/78
NULL Pointer Dereference	19-04-2021	4.3	There is a Null Pointer Dereference in function filter_core/filter_pck.c:gf_filter_pck_new_alloc_internal in GPAC 1.0.1. The pid comes from function av1dmx_parse_flush_sample	https://github.com/gpac/gpac/commit/13dad7d5ef74ca2e6feb4010f5b03eb12e9bbe0e	A-GPA-GPAC-040521/79

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
			, the ctx.opid maybe NULL. The result is a crash in gf_filter_pck_new_alloc_inte rnal. CVE ID : CVE-2021-30015	c	
Out-of- bounds Write	19-04-2021	4.3	In the adts_dmx_process function in filters/reframe_adts.c in GPAC 1.0.1, a crafted file may cause ctx- >hdr.frame_size to be smaller than ctx- >hdr.hdr_size, resulting in size to be a negative number and a heap overflow in the memcpy. CVE ID : CVE-2021-30019	https://github.com/gpac/gpac/commit/22774aa9e62f586319c8f107f5bae950fed900bc	A-GPA- GPAC- 040521/80
Integer Overflow or Wraparound	19-04-2021	4.3	There is a integer overflow in media_tools/av_parsers.c in the gf_avc_read_pps_bs_internal in GPAC 1.0.1. pps_id may be a negative number, so it will not return. However, avc->pps only has 255 unit, so there is an overflow, which results a crash. CVE ID : CVE-2021-30022	https://github.com/gpac/gpac/commit/51cdb67ff7c5f1242ac58c5aa603ceaf1793b788	A-GPA- GPAC- 040521/81
Out-of- bounds Write	19-04-2021	4.3	In the function gf_hevc_read_pps_bs_intern al function in media_tools/av_parsers.c in GPAC 1.0.1 there is a loop, which with crafted file, pps- >num_tile_columns may be larger than sizeof(pps- >column_width), which results in a heap overflow in the loop. CVE ID : CVE-2021-30020	https://github.com/gpac/gpac/commit/51cdb67ff7c5f1242ac58c5aa603ceaf1793b788	A-GPA- GPAC- 040521/82
NULL Pointer	19-04-2021	4.3	The AV1_DuplicateConfig	https://github.com/gpac/gpac/commit/51cdb67ff7c5f1242ac58c5aa603ceaf1793b788	A-GPA-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Dereference			function in GPAC 1.0.1 allows attackers to cause a denial of service (NULL pointer dereference) via a crafted file in the MP4Box command. CVE ID : CVE-2021-31262	ub.com/gpac/gpac/commit/b2eab95e07cb5819375a50358d4806a8813b6e50	GPAC-040521/83					
Integer Overflow or Wraparound	19-04-2021	4.3	There is a integer overflow in media_tools/av_parsers.c in the hevc_parse_slice_segment function in GPAC 1.0.1 which results in a crash. CVE ID : CVE-2021-30014	https://github.com/gpac/gpac/commit/51cdb67ff7c5f1242ac58c5aa603ceaf1793b788	A-GPA-GPAC-040521/84					
NULL Pointer Dereference	19-04-2021	4.3	In filters/reframe_latm.c in GPAC 1.0.1 there is a Null Pointer Dereference, when gf_filter_pck_get_data is called. The first arg pck may be null with a crafted mp4 file,which results in a crash. CVE ID : CVE-2021-30199	https://github.com/gpac/gpac/commit/b2db2f99b4c30f96e17b9a14537c776da6cb5dca	A-GPA-GPAC-040521/85					
Out-of-bounds Write	19-04-2021	6.8	Buffer overflow in the tenc_box_read function in MP4Box in GPAC 1.0.1 allows attackers to cause a denial of service or execute arbitrary code via a crafted file, related invalid IV sizes. CVE ID : CVE-2021-31254	https://github.com/gpac/gpac/commit/8986422c21fbd9a7bf6561cae65aae42077447e8	A-GPA-GPAC-040521/86					
grassroot										
grassroot_platform										
Improper Verification of Cryptographic Signature	19-04-2021	5	Grassroot Platform is an application to make it faster, cheaper and easier to persistently organize and mobilize people in low-income communities. Grassroot Platform before master deployment as of 2021-04-16 did not	https://github.com/grassrootza/grassroot-platform/commit/a2e6e885f8183a066d938cf909fd813a7af7	A-GRA-GRAS-040521/87					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			properly verify the signature of JSON Web Tokens when refreshing an existing JWT. This allows to forge a valid JWT. The problem has been patched in version 1.3.1 by deprecating the JWT refresh function, which was an overdue deprecation regardless (the "refresh" flow is no longer used). CVE ID : CVE-2021-29455	d67f, https://github.com/grasrootza/grasroot-platform/security/advisories/GHSA-f65w-6xw8-6734	
gstreamer_project					
gstreamer					
Use After Free	19-04-2021	6.8	GStreamer before 1.18.4 might access already-freed memory in error code paths when demuxing certain malformed Matroska files. CVE ID : CVE-2021-3497	https://gstreamer.freedesktop.org/security/sa-2021-0002.html , https://bugzilla.redhat.com/show_bug.cgi?id=1945339	A-GST-GSTR-040521/88
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-04-2021	6.8	GStreamer before 1.18.4 might cause heap corruption when parsing certain malformed Matroska files. CVE ID : CVE-2021-3498	https://gstreamer.freedesktop.org/security/sa-2021-0003.html , https://bugzilla.redhat.com/show_bug.cgi?id=1945342	A-GST-GSTR-040521/89
hashicorp					
consul					
N/A	20-04-2021	5	HashiCorp Consul Enterprise version 1.8.0 up	https://www.hashicorp.com	A-HAS-CONS-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			to 1.9.4 audit log can be bypassed by specifically crafted HTTP events. Fixed in 1.9.5, and 1.8.10. CVE ID : CVE-2021-28156	com/blog/category/consul, https://discuss.hashicorp.com/t/hcsec-2021-08-consul-enterprise-audit-log-bypass-for-http-events/23369	040521/90						
terraform_provider											
N/A	22-04-2021	7.5	HashiCorp Terraform's Vault Provider (terraform-provider-vault) did not correctly configure GCE-type bound labels for Vault's GCP auth method. Fixed in 2.19.1. CVE ID : CVE-2021-30476	https://discuss.hashicorp.com/t/hcsec-2021-11-terraform-s-vault-provider-did-not-correctly-configure-bound-labels-for-gcp-auth/23464/2 , https://github.com/hashicorp/terraform-provider-vault/issues/996	A-HAS-TERR-040521/91						
vault											
Improper Certificate Validation	22-04-2021	4.3	HashiCorp Vault and Vault Enterprise 1.5.1 and newer, under certain circumstances, may exclude revoked but unexpired	https://discuss.hashicorp.com/t/hcsec-2021-09-vault-s-pki-	A-HAS-VAUL-040521/92						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			certificates from the CRL. Fixed in 1.5.8, 1.6.4, and 1.7.1. CVE ID : CVE-2021-29653	engine-crl-may-exclude-revoked-but-unexpired-certificates-after-tidy/23461/2	
Improper Certificate Validation	22-04-2021	5	HashiCorp Vault and Vault Enterprise Cassandra integrations (storage backend and database secrets engine plugin) did not validate TLS certificates when connecting to Cassandra clusters. Fixed in 1.6.4 and 1.7.1 CVE ID : CVE-2021-27400	https://discuss.hashicorp.com/t/hcsec-2021-10-vault-s-cassandra-integrations-did-not-validate-tls-certificates/23463	A-HAS-VAUL-040521/93
hornerautomation					
cscape					
Improper Input Validation	23-04-2021	6.8	Cscape (All versions prior to 9.90 SP4) lacks proper validation of user-supplied data when parsing project files. This could lead to memory corruption. An attacker could leverage this vulnerability to execute code in the context of the current process. CVE ID : CVE-2021-22678	N/A	A-HOR-CSCA-040521/94
Improper Access Control	23-04-2021	4.6	Cscape (All versions prior to 9.90 SP4) is configured by default to be installed for all users, which allows full permissions, including read/write access. This may allow unprivileged users to modify the binaries and	N/A	A-HOR-CSCA-040521/95

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			configuration files and lead to local privilege escalation. CVE ID : CVE-2021-22682								
ibm											
informix_dynamic_server											
Out-of-bounds Write	30-04-2021	4.6	IBM Informix Dynamic Server 14.10 is vulnerable to a stack based buffer overflow, caused by improper bounds checking. A local privileged user could overflow a buffer and execute arbitrary code on the system or cause a denial of service condition. IBM X-Force ID: 198366. CVE ID : CVE-2021-20515	https://exchange.xforce.ibmcloud.com/vulnerabilities/198366 , https://www.ibm.com/support/pages/node/6448568	A-IBM-INFO-040521/96						
resilient											
Improper Neutralization of Special Elements used in a Command ('Command Injection')	19-04-2021	6.5	IBM Resilient SOAR V38.0 could allow a privileged user to create create malicious scripts that could be executed as another user. IBM X-Force ID: 198759. CVE ID : CVE-2021-20527	https://www.ibm.com/support/pages/node/6444747 , https://exchange.xforce.ibmcloud.com/vulnerabilities/198759	A-IBM-RESI-040521/97						
spectrum_protect											
Out-of-bounds Write	16-04-2021	2.1	IBM Spectrum Protect Server 7.1 and 8.1 is subject to a stack-based buffer overflow caused by improper bounds checking during the parsing of commands. By issuing such a command with an improper parameter, an authorized administrator could overflow a buffer and	https://exchange.xforce.ibmcloud.com/vulnerabilities/197792 , https://www.ibm.com/support/pages/node/6442993	A-IBM-SPEC-040521/98						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cause the server to crash. IBM X-Force ID: 197792. CVE ID : CVE-2021-20491		
spectrum_protect_backup-archive_client					
Incorrect Default Permissions	26-04-2021	7.2	IBM Spectrum Protect Client 8.1.0.0 through 8.1.11.0 could allow a local user to escalate their privileges to take full control of the system due to insecure directory permissions. IBM X-Force ID: 198811. CVE ID : CVE-2021-20532	https://www.ibm.com/support/pages/node/6445503 , https://exchange.xforce.ibmcloud.com/vulnerabilities/198811	A-IBM-SPEC-040521/99
spectrum_protect_client					
Out-of-bounds Write	26-04-2021	2.1	IBM Spectrum Protect Client 8.1.0.0 through 8.1.11.0 is vulnerable to a stack-based buffer overflow, caused by improper bounds checking. A local attacker could overflow a buffer and cause the application to crash. IBM X-Force ID: 198934 CVE ID : CVE-2021-20546	https://exchange.xforce.ibmcloud.com/vulnerabilities/198934 , https://www.ibm.com/support/pages/node/6445497	A-IBM-SPEC-040521/100
Out-of-bounds Write	26-04-2021	7.2	IBM Spectrum Protect Client 8.1.0.0-8 through 1.11.0 is vulnerable to a stack-based buffer overflow, caused by improper bounds checking when processing the current locale settings. A local attacker could overflow a buffer and execute arbitrary code on the system with elevated privileges or cause the application to crash. IBM X-	https://www.ibm.com/support/pages/node/6445497 , https://exchange.xforce.ibmcloud.com/vulnerabilities/199479	A-IBM-SPEC-040521/101

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			Force ID: 199479 CVE ID : CVE-2021-29672								
spectrum_protect_for_space_management											
Out-of-bounds Write	26-04-2021	2.1	IBM Spectrum Protect Client 8.1.0.0 through 8.1.11.0 is vulnerable to a stack-based buffer overflow, caused by improper bounds checking. A local attacker could overflow a buffer and cause the application to crash. IBM X-Force ID: 198934 CVE ID : CVE-2021-20546	https://exchange.xforce.ibmcloud.com/vulnerabilities/198934 , https://www.ibm.com/support/pages/node/6445497	A-IBM-SPEC-040521/102						
Out-of-bounds Write	26-04-2021	7.2	IBM Spectrum Protect Client 8.1.0.0-8 through 1.11.0 is vulnerable to a stack-based buffer overflow, caused by improper bounds checking when processing the current locale settings. A local attacker could overflow a buffer and execute arbitrary code on the system with elevated privileges or cause the application to crash. IBM X-Force ID: 199479 CVE ID : CVE-2021-29672	https://www.ibm.com/support/pages/node/6445497 , https://exchange.xforce.ibmcloud.com/vulnerabilities/199479	A-IBM-SPEC-040521/103						
spectrum_protect_for_virtual_environments											
Incorrect Default Permissions	26-04-2021	7.2	IBM Spectrum Protect Client 8.1.0.0 through 8.1.11.0 could allow a local user to escalate their privileges to take full control of the system due to insecure directory permissions. IBM X-Force ID: 198811. CVE ID : CVE-2021-20532	https://www.ibm.com/support/pages/node/6445503 , https://exchange.xforce.ibmcloud.com/vulnerabilities/198811	A-IBM-SPEC-040521/104						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
				1						
spectrum_protect_plus										
N/A	26-04-2021	6.4	IBM Spectrum Protect Plus 10.1.0 through 10.1.7 uses Cross-Origin Resource Sharing (CORS) which could allow an attacker to carry out privileged actions and retrieve sensitive information as the domain name is not being limited to only trusted domains. IBM X-Force ID: 196344. CVE ID : CVE-2021-20432	https://exchange.xforce.ibmcloud.com/vulnerabilities/196344, https://www.ibm.com/support/pages/node/6445733	A-IBM-SPEC-040521/105					
Insertion of Sensitive Information into Log File	26-04-2021	2.1	IBM Spectrum Protect Plus File Systems Agent 10.1.6 and 10.1.7 stores potentially sensitive information in log files that could be read by a local user. IBM X-Force ID: 198836. CVE ID : CVE-2021-20536	https://www.ibm.com/support/pages/node/6445739, https://exchange.xforce.ibmcloud.com/vulnerabilities/198836	A-IBM-SPEC-040521/106					
Inadequate Encryption Strength	26-04-2021	5	IBM Spectrum Protect Plus 10.1.0 through 10.1.7 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 200258. CVE ID : CVE-2021-29694	https://exchange.xforce.ibmcloud.com/vulnerabilities/200258, https://www.ibm.com/support/pages/node/6445735	A-IBM-SPEC-040521/107					
websphere_application_server										
Improper Restriction of Recursive Entity References in	20-04-2021	6.4	IBM WebSphere Application Server 8.0, 8.5, and 9.0 is vulnerable to a XML External Entity Injection (XXE) attack when	https://www.ibm.com/support/pages/node/6445171,	A-IBM-WEBS-040521/108					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
DTDs ('XML Entity Expansion')			processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 196648. CVE ID : CVE-2021-20453	https://exchange.xforce.ibmcloud.com/vulnerabilities/196648						
Improper Restriction of XML External Entity Reference	21-04-2021	6.4	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 196649. CVE ID : CVE-2021-20454	https://www.ibm.com/support/pages/node/6445481	A-IBM-WEBS-040521/109					
ivorysearch										
ivory_search										
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2021	4.3	The Search Forms page of the Ivory Search WordPress plugin before 4.6.1 did not properly sanitise the tab parameter before output it in the page, leading to a reflected Cross-Site Scripting issue when opening a malicious crafted link as a high privilege user. Knowledge of a form id is required to conduct the attack. CVE ID : CVE-2021-24234	https://wpscan.com/vulnerability/ec620bec620be-8e29-4860-9d32-86b5814a3835	A-IVO-IVOR-040521/110					
jamovi										
jamovi										
Improper Neutralization	26-04-2021	4.3	Jamovi <=1.6.18 is affected by a cross-site scripting	https://ww	A-JAM-JAMO-					
CVSS Scoring Scale	0-1	1-2	2-3	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 of Input During Web Page Generation ('Cross-site Scripting')			(XSS) vulnerability. The column-name is vulnerable to XSS in the ElectronJS Framework. An attacker can make a .omv (Jamovi) document containing a payload. When opened by victim, the payload is triggered. CVE ID : CVE-2021-28079	w.jamovi.org	040521/111
jenkins					
cloudbees_cd					
Missing Authorization	21-04-2021	4	Jenkins CloudBees CD Plugin 1.1.21 and earlier does not perform a permission check in an HTTP endpoint, allowing attackers with Item/Read permission to schedule builds of projects without having Item/Build permission. CVE ID : CVE-2021-21647	https://www.jenkins.io/security/advisory/2021-04-21/#SECURITY-2309	A-JEN-CLOU-040521/112
config_file_provider					
Improper Restriction of XML External Entity Reference	21-04-2021	5.5	Jenkins Config File Provider Plugin 3.7.0 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks. CVE ID : CVE-2021-21642	https://www.jenkins.io/security/advisory/2021-04-21/#SECURITY-2204	A-JEN-CONF-040521/113
Incorrect Authorization	21-04-2021	4	Jenkins Config File Provider Plugin 3.7.0 and earlier does not correctly perform permission checks in several HTTP endpoints, allowing attackers with global Job/Configure permission to enumerate system-scoped credentials IDs of credentials stored in	https://www.jenkins.io/security/advisory/2021-04-21/#SECURITY-2254	A-JEN-CONF-040521/114

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			Jenkins. CVE ID : CVE-2021-21643								
Cross-Site Request Forgery (CSRF)	21-04-2021	5.8	A cross-site request forgery (CSRF) vulnerability in Jenkins Config File Provider Plugin 3.7.0 and earlier allows attackers to delete configuration files corresponding to an attacker-specified ID. CVE ID : CVE-2021-21644	https://www.jenkins.io/security/advisory/2021-04-21/#SECURITY-2202	A-JEN-CONF-040521/115						
Missing Authorization	21-04-2021	4	Jenkins Config File Provider Plugin 3.7.0 and earlier does not perform permission checks in several HTTP endpoints, attackers with Overall/Read permission to enumerate configuration file IDs. CVE ID : CVE-2021-21645	https://www.jenkins.io/security/advisory/2021-04-21/#SECURITY-2203	A-JEN-CONF-040521/116						
templating_engine											
Protection Mechanism Failure	21-04-2021	6.5	Jenkins Templating Engine Plugin 2.1 and earlier does not protect its pipeline configurations using Script Security Plugin, allowing attackers with Job/Configure permission to execute arbitrary code in the context of the Jenkins controller JVM. CVE ID : CVE-2021-21646	https://www.jenkins.io/security/advisory/2021-04-21/#SECURITY-2311	A-JEN-TEMP-040521/117						
jhead_project											
jhead											
Out-of-bounds Write	22-04-2021	6.8	A heap-based buffer overflow was found in jhead in version 3.06 in Get16u() in exif.c when processing a crafted file. CVE ID : CVE-2021-3496	https://github.com/Mattias-Wandel/jhead/issues/33	A-JHE-JHEA-040521/118						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
jose_project					
jose					
Observable Discrepancy	16-04-2021	4.3	jose is an npm library providing a number of cryptographic operations. In vulnerable versions AES_CBC_HMAC_SHA2 Algorithm (A128CBC-HS256, A192CBC-HS384, A256CBC-HS512) decryption would always execute both HMAC tag verification and CBC decryption, if either failed `JWE decryption failed` would be thrown. A possibly observable difference in timing when padding error would occur while decrypting the ciphertext makes a padding oracle and an adversary might be able to make use of that oracle to decrypt data without knowing the decryption key by issuing on average $128 \cdot b$ calls to the padding oracle (where b is the number of bytes in the ciphertext block). All major release versions have had a patch released which ensures the HMAC tag is verified before performing CBC decryption. The fixed versions are `^1.28.1 ^2.0.5 >=3.11.4`. Users should upgrade their v1.x dependency to ^1.28.1, their v2.x dependency to ^2.0.5, and their v3.x dependency to ^3.11.4. Thanks to Jason from	https://github.com/paiva/jose/security/advisories/GHSA-58f5-hfqc-jgch	A-JOS-JOSE-040521/119

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Microsoft Vulnerability Research (MSVR) for bringing this up and Eva Sarafianou (@esarafianou) for helping to score this advisory. CVE ID : CVE-2021-29443		
Observable Discrepancy	16-04-2021	4.3	jose-node-esm-runtime is an npm package which provides a number of cryptographic functions. In versions prior to 3.11.4 the AES_CBC_HMAC_SHA2 Algorithm (A128CBC-HS256, A192CBC-HS384, A256CBC-HS512) decryption would always execute both HMAC tag verification and CBC decryption, if either failed `JWEDecryptionFailed` would be thrown. But a possibly observable difference in timing when padding error would occur while decrypting the ciphertext makes a padding oracle and an adversary might be able to make use of that oracle to decrypt data without knowing the decryption key by issuing on average $128 \cdot b$ calls to the padding oracle (where b is the number of bytes in the ciphertext block). A patch was released which ensures the HMAC tag is verified before performing CBC decryption. The fixed versions are `>=3.11.4`. Users should upgrade to `^3.11.4`.	https://github.com/paiva/jose/security/advisories/GHSA-4v4g-726h-xvfv	A-JOS-JOSE-040521/120

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-29445		
Observable Discrepancy	16-04-2021	4.3	jose-browser-runtime is an npm package which provides a number of cryptographic functions. In versions prior to 3.11.4 the AES_CBC_HMAC_SHA2 Algorithm (A128CBC-HS256, A192CBC-HS384, A256CBC-HS512) decryption would always execute both HMAC tag verification and CBC decryption, if either failed `JWE decryption failed` would be thrown. But a possibly observable difference in timing when padding error would occur while decrypting the ciphertext makes a padding oracle and an adversary might be able to make use of that oracle to decrypt data without knowing the decryption key by issuing on average $128 \cdot b$ calls to the padding oracle (where b is the number of bytes in the ciphertext block). A patch was released which ensures the HMAC tag is verified before performing CBC decryption. The fixed versions are `>=3.11.4`. Users should upgrade to `^3.11.4`.	https://github.com/panva/jose/security/advisories/GHSA-94hh-pjjg-rwmr	A-JOS-JOSE-040521/121
Observable Discrepancy	16-04-2021	4.3	jose-node-cjs-runtime is an npm package which provides a number of cryptographic functions. In versions prior to 3.11.4 the	https://github.com/panva/jose/security/advisories/GHSA-	A-JOS-JOSE-040521/122

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>AES_CBC_HMAC_SHA2 Algorithm (A128CBC-HS256, A192CBC-HS384, A256CBC-HS512) decryption would always execute both HMAC tag verification and CBC decryption, if either failed `JWEDecryptionFailed` would be thrown. But a possibly observable difference in timing when padding error would occur while decrypting the ciphertext makes a padding oracle and an adversary might be able to make use of that oracle to decrypt data without knowing the decryption key by issuing on average $128 \cdot b$ calls to the padding oracle (where b is the number of bytes in the ciphertext block). A patch was released which ensures the HMAC tag is verified before performing CBC decryption. The fixed versions are `>=3.11.4`. Users should upgrade to `^3.11.4`.</p> <p>CVE ID : CVE-2021-29446</p>	rvcw-f68w-8h8h	
jquery-bbq_project					
jquery-bbq					
N/A	23-04-2021	7.5	<p>Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in jquery-bbq 1.2.1 allows a malicious user to inject properties into Object.prototype.</p>	N/A	A-JQU-JQUE-040521/123

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-20086		
jquery-plugin-query-object_project					
jquery-plugin-query-object					
N/A	23-04-2021	6.5	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in jquery-plugin-query-object 2.2.3 allows a malicious user to inject properties into Object.prototype. CVE ID : CVE-2021-20083	N/A	A-JQU-JQUE-040521/124
jquery-sparkle_project					
jquery-sparkle					
N/A	23-04-2021	6.5	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in jquery-sparkle 1.5.2-beta allows a malicious user to inject properties into Object.prototype. CVE ID : CVE-2021-20084	N/A	A-JQU-JQUE-040521/125
juniper					
paragon_active_assurance_control_center					
Exposure of Resource to Wrong Sphere	22-04-2021	5.8	An authentication bypass vulnerability in the Juniper Networks Paragon Active Assurance Control Center may allow an attacker with specific information about the deployment to mimic an already registered Test Agent and access its configuration including associated inventory details. If the issue occurs, the affected Test Agent will not be able to connect to the Control Center. This issue	https://kb.juniper.net/JS_A11127	A-JUN-PARA-040521/126

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affects Juniper Networks Paragon Active Assurance Control Center All versions prior to 2.35.6; 2.36 versions prior to 2.36.2. CVE ID : CVE-2021-0232		
vsrx					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-04-2021	6.8	A path traversal vulnerability in the Juniper Networks SRX and vSRX Series may allow an authenticated J-web user to read sensitive system files. This issue affects Juniper Networks Junos OS on SRX and vSRX Series: 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R2-S4, 19.4R3; 20.1 versions prior to 20.1R1-S4, 20.1R2; 20.2 versions prior to 20.2R1-S3, 20.2R2; This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1. CVE ID : CVE-2021-0231	https://kb.juniper.net/JS_A11126	A-JUN-VSRX-040521/127
killig_project					
killig					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-04-2021	7.5	This affects all versions of package killing. If attacker-controlled user input is given, it is possible for an attacker to execute arbitrary commands. This is due to use of the child_process exec function without input sanitization. CVE ID : CVE-2021-23381	N/A	A-KIL-KILL-040521/128
lstudio					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
restructuredtext					
Incorrect Authorization	20-04-2021	7.5	vscode-restructuredtext before 146.0.0 contains an incorrect access control vulnerability, where a crafted project folder could execute arbitrary binaries via crafted workspace configuration. CVE ID : CVE-2021-28793	https://github.com/vscode-restructuredtext/vscode-restructuredtext/commit/1dd3e878a5559e3dfe0e48f145c90418b208c5af	A-LEX-REST-040521/129
libtpms_project					
libtpms					
Insufficient Entropy	19-04-2021	2.1	A flaw was found in libtpms in versions before 0.8.0. The TPM 2 implementation returns 2048 bit keys with ~1984 bit strength due to a bug in the TCG specification. The bug is in the key creation algorithm in RsaAdjustPrimeCandidate(), which is called before the prime number check. The highest threat from this vulnerability is to data confidentiality. CVE ID : CVE-2021-3505	https://bugzilla.redhat.com/show_bug.cgi?id=1950046 , https://github.com/stefanberger/libtpms/issues/183	A-LIB-LIBT-040521/130
manta					
safe-obj					
N/A	26-04-2021	7.5	Prototype pollution vulnerability in 'safe-obj' versions 1.0.0 through 1.0.2 allows an attacker to cause a denial of service and may lead to remote code execution. CVE ID : CVE-2021-25928	N/A	A-MAN-SAFE-040521/131

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
manydesigns					
portofino					
Improper Verification of Cryptographic Signature	16-04-2021	6.4	Portofino is an open source web development framework. Portofino before version 5.2.1 did not properly verify the signature of JSON Web Tokens. This allows forging a valid JWT. The issue will be patched in the upcoming 5.2.1 release. CVE ID : CVE-2021-29451	https://github.com/ManyDesigns/Portofino/security/advisories/GHSA-6g3c-2mh5-7q6x , https://github.com/ManyDesigns/Portofino/commit/8c754a0ad234555e813dcbf9e57d637f9f23d8fb	A-MAN-PORT-040521/132
matrix-media-repo_project					
matrix-media-repo					
Uncontrolled Resource Consumption	19-04-2021	4	matrix-media-repo is an open-source multi-domain media repository for Matrix. Versions 1.2.6 and earlier of matrix-media-repo do not properly handle malicious images which are crafted to be small in file size, but large in complexity. A malicious user could upload a relatively small image in terms of file size, using particular image formats, which expands to have extremely large dimensions during the process of thumbnailing. The server can be exhausted of memory in the process of trying to load the whole image into memory for	https://github.com/turtlelive/matrix-media-repo/security/advisories/GHSA-j889-h476-hh9h	A-MAT-MATR-040521/133

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			thumbnailing, leading to denial of service. Version 1.2.7 has a fix for the vulnerability. CVE ID : CVE-2021-29453		
mediawiki					
mediawiki					
Exposure of Resource to Wrong Sphere	22-04-2021	4	An issue was discovered in the AbuseFilter extension for MediaWiki through 1.35.2. Its AbuseFilterCheckMatch API reveals suppressed edits and usernames to unprivileged users through the iteration of crafted AbuseFilter rules. CVE ID : CVE-2021-31547	N/A	A-MED-MEDI-040521/134
Exposure of Resource to Wrong Sphere	22-04-2021	4	An issue was discovered in the AbuseFilter extension for MediaWiki through 1.35.2. A MediaWiki user who is partially blocked or was unsuccessfully blocked could bypass AbuseFilter and have their edits completed. CVE ID : CVE-2021-31548	N/A	A-MED-MEDI-040521/135
Exposure of Sensitive Information to an Unauthorized Actor	22-04-2021	4	An issue was discovered in the AbuseFilter extension for MediaWiki through 1.35.2. The Special:AbuseFilter/examine form allowed for the disclosure of suppressed MediaWiki usernames to unprivileged users. CVE ID : CVE-2021-31549	https://gerri.t.wikimedia.org/r/q/I71a6d521bd12931ce60eec4d2dc35af19146000f , https://gerri.t.wikimedia.org/r/q/I6063c02fa261c4cc0e6dbbb2db4e111eb	A-MED-MEDI-040521/136

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
				85912c2	
Exposure of Resource to Wrong Sphere	22-04-2021	5.5	<p>An issue was discovered in the AbuseFilter extension for MediaWiki through 1.35.2. It incorrectly executed certain rules related to blocking accounts after account creation. Such rules would allow for user accounts to be created while blocking only the IP address used to create an account (and not the user account itself). Such rules could also be used by a nefarious, unprivileged user to catalog and enumerate any number of IP addresses related to these account creations.</p> <p>CVE ID : CVE-2021-31552</p>	https://gerri.t.wikimedia.org/r/q/I8bae477ad7e4d0190335363ac2decf28e4313da1	A-MED-MEDI-040521/137
Exposure of Resource to Wrong Sphere	22-04-2021	5.5	<p>An issue was discovered in the AbuseFilter extension for MediaWiki through 1.35.2. It improperly handled account blocks for certain automatically created MediaWiki user accounts, thus allowing nefarious users to remain unblocked.</p> <p>CVE ID : CVE-2021-31554</p>	https://gerri.t.wikimedia.org/r/q/Ie1f4333d5b1c9d17fb2236fe38a31de427a4cc48	A-MED-MEDI-040521/138
Improper Input Validation	22-04-2021	5	<p>An issue was discovered in the Oauth extension for MediaWiki through 1.35.2. It did not validate the oarc_version (aka oauth_registered_consumer.oarc_version) parameter's length.</p> <p>CVE ID : CVE-2021-31555</p>	https://gerri.t.wikimedia.org/r/q/I222c053b4b14ac1ad0f5b3a51565b1b9cd4c139d	A-MED-MEDI-040521/139

CVSS Scoring Scale	0-1	1-2	2-3	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 of Sensitive Information to an Unauthorized Actor	22-04-2021	4	An issue was discovered in the AbuseFilter extension for MediaWiki through 1.35.2. It incorrectly logged sensitive suppression deletions, which should not have been visible to users with access to view AbuseFilter log data. CVE ID : CVE-2021-31546	N/A	A-MED-MEDI-040521/140
Exposure of Sensitive Information to an Unauthorized Actor	22-04-2021	5	An issue was discovered in the AbuseFilter extension for MediaWiki through 1.35.2. The page_recent_contributors leaked the existence of certain deleted MediaWiki usernames, related to rev_deleted. CVE ID : CVE-2021-31545	https://gerri.t.wikimedia.org/r/q/I8d5ed9ca84282ee50832035af86123633fc88293	A-MED-MEDI-040521/141
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2021	3.5	An issue was discovered in the CommentBox extension for MediaWiki through 1.35.2. Via crafted configuration variables, a malicious actor could introduce XSS payloads into various layers. CVE ID : CVE-2021-31550	https://gerri.t.wikimedia.org/r/c/mediawiki/extensions/Commentbox/+/651934/	A-MED-MEDI-040521/142
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2021	4.3	An issue was discovered in the PageForms extension for MediaWiki through 1.35.2. Crafted payloads for Token-related query parameters allowed for XSS on certain PageForms-managed MediaWiki pages. CVE ID : CVE-2021-31551	N/A	A-MED-MEDI-040521/143
Unquoted Search Path or Element	22-04-2021	6.4	An issue was discovered in the CheckUser extension for MediaWiki through 1.35.2.	N/A	A-MED-MEDI-040521/144

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>MediaWiki usernames with trailing whitespace could be stored in the cu_log database table such that denial of service occurred for certain CheckUser extension pages and functionality. For example, the attacker could turn off Special:CheckUserLog and thus interfere with usage tracking.</p> <p>CVE ID : CVE-2021-31553</p>		

mendix

mendix

Improper Privilege Management	16-04-2021	6.5	<p>A vulnerability has been identified in Mendix Applications using Mendix 7 (All versions < V7.23.19), Mendix Applications using Mendix 8 (All versions < V8.17.0), Mendix Applications using Mendix 8 (V8.12) (All versions < V8.12.5), Mendix Applications using Mendix 8 (V8.6) (All versions < V8.6.9), Mendix Applications using Mendix 9 (All versions < V9.0.5). Authenticated, non-administrative users could modify their privileges by manipulating the user role under certain circumstances, allowing them to gain administrative privileges.</p> <p>CVE ID : CVE-2021-27394</p>	https://cert-portal.siemens.com/productcert/pdf/ssa-875726.pdf	A-MEN-MEND-040521/145
-------------------------------	------------	-----	---	---	-----------------------

minthcm

minthcm

CVSS Scoring Scale	0-1	1-2	2-3	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')	26-04-2021	4.3	The Import function in MintHCM RELEASE 3.0.8 allows an attacker to execute a cross-site scripting (XSS) payload in file-upload. CVE ID : CVE-2021-25838	https://mint-hcm.org/	A-MIN-MINT-040521/146
mootools					
mootools-more					
N/A	23-04-2021	6.5	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in mootools-more 1.6.0 allows a malicious user to inject properties into Object.prototype. CVE ID : CVE-2021-20088	N/A	A-MOO-MOOT-040521/147
nvidia					
geforce_experience					
N/A	20-04-2021	4.6	NVIDIA GeForce Experience, all versions prior to 3.22, contains a vulnerability in GameStream plugins where log files are created using NT/System level permissions, which may lead to code execution, denial of service, or local privilege escalation. CVE ID : CVE-2021-1079	https://nvidia.custhelp.com/app/answers/detail/a_id/5184	A-NVI-GEFO-040521/148
omicronenergy					
stationguard					
Uncontrolled Resource Consumption	20-04-2021	5	OMICRON StationGuard before 1.10 allows remote attackers to cause a denial of service (connectivity outage) via crafted	https://www.omicronenergy.com/download/file/e81f23250	A-OMI-STAT-040521/149

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			tcp/20499 packets to the CTRL Ethernet port. CVE ID : CVE-2021-30464	097e7d5e1071dfbdb7f16d2/, https://www.omicronenergy.com/en/support/product-security/	
onion-oled-js_project					
onion-oled-js					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-04-2021	7.5	This affects all versions of package onion-oled-js. If attacker-controlled user input is given to the scroll function, it is possible for an attacker to execute arbitrary commands. This is due to use of the child_process exec function without input sanitization. CVE ID : CVE-2021-23377	N/A	A-ONI-ONIO-040521/150
openmage					
magento					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-04-2021	6.5	Magento-lts is a long-term support alternative to Magento Community Edition (CE). A vulnerability in magento-lts versions before 19.4.13 and 20.0.9 potentially allows an administrator unauthorized access to restricted resources. This is a backport of CVE-2021-21024. The vulnerability is patched in versions 19.4.13 and 20.0.9. CVE ID : CVE-2021-21427	https://github.com/OpenMage/magento-lts/security/advisories/GHSA-fvrf-9428-527m	A-OPE-MAGE-040521/151
Deserialization of	21-04-2021	7.5	Magento-lts is a long-term support alternative to	https://github.com/OpenMage/magento-lts/security/advisories/GHSA-fvrf-9428-527m	A-OPE-MAGE-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
Untrusted Data			Magento Community Edition (CE). In magento-lts versions 19.4.12 and prior and 20.0.8 and prior, there is a vulnerability caused by the unsecured deserialization of an object. A patch in versions 19.4.13 and 20.0.9 was back ported from Zend Framework 3. The vulnerability was assigned CVE-2021-3007 in Zend Framework. CVE ID : CVE-2021-21426	nMage/magento-lts/security/advisories/GHSA-m496-x567-f98c	040521/152						
oracle											
advanced_collections											
N/A	22-04-2021	5.5	Vulnerability in the Oracle Advanced Collections product of Oracle E-Business Suite (component: Admin). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Advanced Collections. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Advanced Collections accessible data as well as unauthorized access to critical data or complete access to all Oracle Advanced Collections accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-ADVA-040521/153						
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						
			Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). CVE ID : CVE-2021-2247								
advanced_pricing											
N/A	22-04-2021	5.5	Vulnerability in the Oracle Advanced Pricing product of Oracle E-Business Suite (component: Price Book). The supported version that is affected is 12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Advanced Pricing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Advanced Pricing accessible data as well as unauthorized access to critical data or complete access to all Oracle Advanced Pricing accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). CVE ID : CVE-2021-2269	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-ADVA-040521/154						
advanced_supply_chain_planning											
N/A	22-04-2021	6.4	Vulnerability in the Oracle Advanced Supply Chain Planning product of Oracle Supply Chain (component: Core). Supported versions	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-ADVA-040521/155						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that are affected are 12.1 and 12.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Advanced Supply Chain Planning. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Advanced Supply Chain Planning accessible data as well as unauthorized access to critical data or complete access to all Oracle Advanced Supply Chain Planning accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N). CVE ID : CVE-2021-2253		
application_object_library					
N/A	22-04-2021	5.5	Vulnerability in the Oracle Application Object Library product of Oracle E-Business Suite (component: Profiles). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Application Object Library. Successful attacks of this vulnerability can result in	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-APPL-040521/156

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>unauthorized creation, deletion or modification access to critical data or all Oracle Application Object Library accessible data as well as unauthorized access to critical data or complete access to all Oracle Application Object Library accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).</p> <p>CVE ID : CVE-2021-2314</p>		

applications_framework

N/A	22-04-2021	6.4	<p>Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Home page). The supported version that is affected is 12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Framework. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Applications Framework accessible data as well as unauthorized access to critical data or complete access to all Oracle Applications Framework accessible data. CVSS 3.1 Base Score 9.1</p>	<p>https://www.oracle.com/security-alerts/cpuapr2021.html</p>	A-ORA-APPL-040521/157
-----	------------	-----	---	--	-----------------------

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					
			(Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N). CVE ID : CVE-2021-2200							
applications_manager										
N/A	22-04-2021	5.5	Vulnerability in the Oracle Applications Manager product of Oracle E-Business Suite (component: View Reports). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Applications Manager. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Applications Manager accessible data as well as unauthorized access to critical data or complete access to all Oracle Applications Manager accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N). CVE ID : CVE-2021-2275	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-APPL-040521/158					
bill_presentment_architecture										
N/A	22-04-2021	5.5	Vulnerability in the Oracle Bill Presentment	https://www.oracle.com	A-ORA-BILL-040521/159					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Architecture product of Oracle E-Business Suite (component: Template Search). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Bill Presentment Architecture. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Bill Presentment Architecture accessible data as well as unauthorized access to critical data or complete access to all Oracle Bill Presentment Architecture accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).</p> <p>CVE ID : CVE-2021-2222</p>	m/security-alerts/cpuap r2021.html	

bills_of_material

N/A	22-04-2021	5.5	<p>Vulnerability in the Oracle Bills of Material product of Oracle E-Business Suite (component: Bill Issues). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Bills of</p>	https://www.oracle.com/security-alerts/cpuap r2021.html	A-ORA-BILL-040521/160
-----	------------	-----	--	---	-----------------------

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
			<p>Material. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Bills of Material accessible data as well as unauthorized access to critical data or complete access to all Oracle Bills of Material accessible data.</p> <p>CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).</p> <p>CVE ID : CVE-2021-2288</p>		

business_intelligence

N/A	22-04-2021	4.9	<p>Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Actions). Supported versions that are affected are 5.5.0.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-BUSI-040521/161
-----	------------	-----	--	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).</p> <p>CVE ID : CVE-2021-2191</p>		
N/A	22-04-2021	3.6	<p>Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: Analytics Web General). Supported versions that are affected are 5.5.0.0.0, 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-BUSI-040521/162

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 4.0 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:C/C:L/I:L/A:N).</p> <p>CVE ID : CVE-2021-2152</p>		

cash_management

N/A	22-04-2021	5.5	<p>Vulnerability in the Oracle Cash Management product of Oracle E-Business Suite (component: Bank Account Transfer). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Cash Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Cash Management accessible data as well as unauthorized access to critical data or complete</p>	<p>https://www.oracle.com/security-alerts/cpuapr2021.html</p>	A-ORA-CASH-040521/163
-----	------------	-----	---	--	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to all Oracle Cash Management accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). CVE ID : CVE-2021-2227		
cloud_infrastructure_storage_gateway					
N/A	22-04-2021	6.5	Vulnerability in the Oracle Cloud Infrastructure Storage Gateway product of Oracle Storage Gateway (component: Management Console). The supported version that is affected is Prior to 1.4. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Cloud Infrastructure Storage Gateway. While the vulnerability is in Oracle Cloud Infrastructure Storage Gateway, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Cloud Infrastructure Storage Gateway. Note: Updating the Oracle Cloud Infrastructure Storage Gateway to version 1.4 or later will address these vulnerabilities. Download the latest version of Oracle Cloud Infrastructure Storage Gateway from <a	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-CLOU-040521/164

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			https://www.oracle.com/downloads/cloud/oci-storage-gateway-downloads.html ">here. Refer to Document 2768897.1 for more details. CVSS 3.1 Base Score 9.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H). CVE ID : CVE-2021-2319		
N/A	22-04-2021	7.5	Vulnerability in the Oracle Cloud Infrastructure Storage Gateway product of Oracle Storage Gateway (component: Management Console). The supported version that is affected is Prior to 1.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Cloud Infrastructure Storage Gateway. While the vulnerability is in Oracle Cloud Infrastructure Storage Gateway, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Cloud Infrastructure Storage Gateway. Note: Updating the Oracle Cloud Infrastructure Storage	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-CLOU-040521/165

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
			<p>Gateway to version 1.4 or later will address these vulnerabilities. Download the latest version of Oracle Cloud Infrastructure Storage Gateway from https://www.oracle.com/downloads/cloud/oci-storage-gateway-downloads.html here. Refer to Document https://support.oracle.com/rs?type=doc&id=2768897.1 for more details. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).</p> <p>CVE ID : CVE-2021-2317</p>		
N/A	22-04-2021	6.5	<p>Vulnerability in the Oracle Cloud Infrastructure Storage Gateway product of Oracle Storage Gateway (component: Management Console). The supported version that is affected is Prior to 1.4. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Cloud Infrastructure Storage Gateway. While the vulnerability is in Oracle Cloud Infrastructure Storage Gateway, attacks may significantly impact additional products. Successful attacks of this</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-CLOU-040521/166

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerability can result in takeover of Oracle Cloud Infrastructure Storage Gateway. Note: Updating the Oracle Cloud Infrastructure Storage Gateway to version 1.4 or later will address these vulnerabilities. Download the latest version of Oracle Cloud Infrastructure Storage Gateway from https://www.oracle.com/downloads/cloud/oci-storage-gateway-downloads.html here. Refer to Document https://support.oracle.com/rs?type=doc&id=2768897.1 for more details. CVSS 3.1 Base Score 9.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).</p> <p>CVE ID : CVE-2021-2318</p>		
N/A	22-04-2021	6.5	<p>Vulnerability in the Oracle Cloud Infrastructure Storage Gateway product of Oracle Storage Gateway (component: Management Console). The supported version that is affected is Prior to 1.4. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Cloud Infrastructure Storage Gateway. While the</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-CLOU-040521/167

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerability is in Oracle Cloud Infrastructure Storage Gateway, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Cloud Infrastructure Storage Gateway. Note: Updating the Oracle Cloud Infrastructure Storage Gateway to version 1.4 or later will address these vulnerabilities. Download the latest version of Oracle Cloud Infrastructure Storage Gateway from https://www.oracle.com/downloads/cloud/oci-storage-gateway-downloads.html here. Refer to Document https://support.oracle.com/rs?type=doc&id=2768897.1 for more details. CVSS 3.1 Base Score 9.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).</p> <p>CVE ID : CVE-2021-2320</p>		
coherence					
N/A	22-04-2021	5	<p>Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 3.7.1.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0.</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-COHE-040521/168

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Coherence. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Coherence accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). CVE ID : CVE-2021-2277		

compensation_workbench

N/A	22-04-2021	5.5	Vulnerability in the Oracle Compensation Workbench product of Oracle E-Business Suite (component: Compensation Workbench). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Compensation Workbench. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Compensation Workbench accessible data as well as unauthorized access to critical data or complete access to all Oracle Compensation Workbench accessible data.	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-COMP-040521/169
-----	------------	-----	---	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). CVE ID : CVE-2021-2224		
concurrent_processing					
N/A	22-04-2021	5.5	Vulnerability in the Oracle Concurrent Processing product of Oracle E-Business Suite (component: BI Publisher Integration). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Concurrent Processing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Concurrent Processing accessible data as well as unauthorized access to critical data or complete access to all Oracle Concurrent Processing accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). CVE ID : CVE-2021-2295	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-CONC-040521/170
crm_technical_foundation					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	22-04-2021	5.5	<p>Vulnerability in the Oracle CRM Technical Foundation product of Oracle E-Business Suite (component: Data Source). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle CRM Technical Foundation accessible data as well as unauthorized access to critical data or complete access to all Oracle CRM Technical Foundation accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).</p> <p>CVE ID : CVE-2021-2251</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-CRM_-040521/171
customers_online					
N/A	22-04-2021	5.5	<p>Vulnerability in the Oracle Customers Online product of Oracle E-Business Suite (component: Customer Tab). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-CUST-040521/172

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access via HTTP to compromise Oracle Customers Online. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Customers Online accessible data as well as unauthorized access to critical data or complete access to all Oracle Customers Online accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). CVE ID : CVE-2021-2156		
database					
N/A	22-04-2021	4	Vulnerability in the Oracle Database - Enterprise Edition Unified Audit component of Oracle Database Server. Supported versions that are affected are 18c and 19c. Easily exploitable vulnerability allows high privileged attacker having Create Audit Policy privilege with network access via Oracle Net to compromise Oracle Database - Enterprise Edition Unified Audit. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Database -	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-DATA-040521/173

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Edition Unified Audit accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N). CVE ID : CVE-2021-2245		
N/A	22-04-2021	2.1	Vulnerability in the Oracle Database - Enterprise Edition component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows high privileged attacker having RMAN executable privilege with logon to the infrastructure where Oracle Database - Enterprise Edition executes to compromise Oracle Database - Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Database - Enterprise Edition accessible data. CVSS 3.1 Base Score 2.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N). CVE ID : CVE-2021-2207	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-DATA-040521/174
database_server					
N/A	22-04-2021	4	Vulnerability in the Recovery component of Oracle Database Server. Supported versions that are affected are 12.1.0.2,	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-DATA-040521/175

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows high privileged attacker having DBA Level Account privilege with network access via Oracle Net to compromise Recovery. While the vulnerability is in Recovery, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Recovery accessible data. CVSS 3.1 Base Score 4.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N). CVE ID : CVE-2021-2173		
N/A	22-04-2021	3.5	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows low privileged attacker having Create Session privilege with network access via Oracle Net to compromise Java VM. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java VM accessible data. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-DATA-040521/176

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			/UI:N/S:U/C:N/I:H/A:N). CVE ID : CVE-2021-2234		
N/A	22-04-2021	4	Vulnerability in the Database Vault component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows high privileged attacker having Create Any View, Select Any View privilege with network access via Oracle Net to compromise Database Vault. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Database Vault accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N). CVE ID : CVE-2021-2175	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-DATA-040521/177
depot_repair					
N/A	22-04-2021	5.5	Vulnerability in the Oracle Depot Repair product of Oracle E-Business Suite (component: LOVs). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Depot Repair. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-DEPO-040521/178

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to critical data or all Oracle Depot Repair accessible data as well as unauthorized access to critical data or complete access to all Oracle Depot Repair accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). CVE ID : CVE-2021-2229		

document_management_and_collaboration

N/A	22-04-2021	5.5	Vulnerability in the Oracle Document Management and Collaboration product of Oracle E-Business Suite (component: Document Management). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Document Management and Collaboration. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Document Management and Collaboration accessible data as well as unauthorized access to critical data or complete access to all Oracle Document Management and	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-DOCU-040521/179
-----	------------	-----	--	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Collaboration accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).</p> <p>CVE ID : CVE-2021-2292</p>		
N/A	22-04-2021	5.5	<p>Vulnerability in the Oracle Document Management and Collaboration product of Oracle E-Business Suite (component: Attachments). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Document Management and Collaboration. While the vulnerability is in Oracle Document Management and Collaboration, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Document Management and Collaboration accessible data as well as unauthorized update, insert or delete access to some of Oracle Document Management and Collaboration accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and</p>	<p>https://www.oracle.com/security-alerts/cpuapr2021.html</p>	A-ORA-DOCU-040521/180

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H /UI:N/S:C/C:H/I:L/A:N). CVE ID : CVE-2021-2181								
e-business_intelligence											
N/A	22-04-2021	5.5	Vulnerability in the Oracle E-Business Intelligence product of Oracle E-Business Suite (component: DBI Setups). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle E-Business Intelligence. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle E-Business Intelligence accessible data as well as unauthorized access to critical data or complete access to all Oracle E-Business Intelligence accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L /UI:N/S:U/C:H/I:H/A:N). CVE ID : CVE-2021-2225	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-E-BU-040521/181						
e-business_tax											
N/A	22-04-2021	5.5	Vulnerability in the Oracle E-Business Tax product of Oracle E-Business Suite	https://www.oracle.com/security-	A-ORA-E-BU-040521/182						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(component: User Interface). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle E-Business Tax. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle E-Business Tax accessible data as well as unauthorized access to critical data or complete access to all Oracle E-Business Tax accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). CVE ID : CVE-2021-2274	alerts/cpuap r2021.html	

email_center

N/A	22-04-2021	5.5	Vulnerability in the Oracle Email Center product of Oracle E-Business Suite (component: Message Display). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Email	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-EMAI-040521/183
-----	------------	-----	--	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Center. While the vulnerability is in Oracle Email Center, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Email Center accessible data as well as unauthorized update, insert or delete access to some of Oracle Email Center accessible data. CVSS 3.1 Base Score 8.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N). CVE ID : CVE-2021-2209		
engineering					
N/A	22-04-2021	5.5	Vulnerability in the Oracle Engineering product of Oracle E-Business Suite (component: Change Management). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Engineering. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Engineering accessible data	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-ENGI-040521/184

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			as well as unauthorized access to critical data or complete access to all Oracle Engineering accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). CVE ID : CVE-2021-2290		
enterprise_asset_management					
N/A	22-04-2021	5.5	Vulnerability in the Oracle Enterprise Asset Management product of Oracle E-Business Suite (component: Setup). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Asset Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Enterprise Asset Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Enterprise Asset Management accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-ENTE-040521/185

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). CVE ID : CVE-2021-2233								
enterprise_manager											
N/A	22-04-2021	7.5	Vulnerability in the Enterprise Manager for Fusion Middleware product of Oracle Enterprise Manager (component: FMW Control Plugin). The supported version that is affected are 11.1.1.9 and 12.2.1.3 Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Enterprise Manager for Fusion Middleware. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Enterprise Manager for Fusion Middleware accessible data as well as unauthorized read access to a subset of Enterprise Manager for Fusion Middleware accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Enterprise Manager for Fusion Middleware. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-ENTE-040521/186						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			CVE ID : CVE-2021-2008								
N/A	22-04-2021	4	Vulnerability in the Enterprise Manager for Fusion Middleware product of Oracle Enterprise Manager (component: FMW Control Plugin). The supported version that is affected is 12.2.1.4. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Enterprise Manager for Fusion Middleware. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Enterprise Manager for Fusion Middleware. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2021-2134	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-ENTE-040521/187						
enterprise_manager_base_platform											
N/A	22-04-2021	5.8	Vulnerability in the Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: UI Framework). The supported version that is affected is 13.4.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Enterprise Manager Base	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-ENTE-040521/188						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Platform. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Enterprise Manager Base Platform, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Enterprise Manager Base Platform accessible data as well as unauthorized read access to a subset of Enterprise Manager Base Platform accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). CVE ID : CVE-2021-2053		
financial_services_analytical_applications_infrastructure					
N/A	22-04-2021	5.8	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure product of Oracle Financial Services Applications (component: Rules Framework). Supported versions that are affected are 8.0.6-8.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-FINA-040521/189

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Infrastructure. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Financial Services Analytical Applications Infrastructure, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Analytical Applications Infrastructure accessible data as well as unauthorized read access to a subset of Oracle Financial Services Analytical Applications Infrastructure accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).</p> <p>CVE ID : CVE-2021-2140</p>		
financials_common_modules					
N/A	22-04-2021	5.5	<p>Vulnerability in the Oracle Financials Common Modules product of Oracle E-Business Suite (component: Advanced Global Intercompany). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-FINA-040521/190

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>compromise Oracle Financials Common Modules. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financials Common Modules accessible data as well as unauthorized access to critical data or complete access to all Oracle Financials Common Modules accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).</p> <p>CVE ID : CVE-2021-2236</p>		

flexcube_direct_banking

N/A	22-04-2021	2.1	<p>Vulnerability in the Oracle FLEXCUBE Direct Banking product of Oracle Financial Services Applications (component: Pre Login). Supported versions that are affected are 12.0.2 and 12.0.3. Difficult to exploit vulnerability allows high privileged attacker with network access via Oracle Net to compromise Oracle FLEXCUBE Direct Banking. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete</p>	<p>https://www.oracle.com/security-alerts/cpuapr2021.html</p>	A-ORA-FLEX-040521/191
-----	------------	-----	---	--	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			access to some of Oracle FLEXCUBE Direct Banking accessible data. CVSS 3.1 Base Score 2.0 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:N). CVE ID : CVE-2021-2141							
general_ledger										
N/A	22-04-2021	5.5	Vulnerability in the Oracle General Ledger product of Oracle E-Business Suite (component: Account Hierarchy Manager). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle General Ledger. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle General Ledger accessible data as well as unauthorized access to critical data or complete access to all Oracle General Ledger accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). CVE ID : CVE-2021-2237	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-GENE-040521/192					
hospitality_inventory_management										
N/A	22-04-2021	4	Vulnerability in the Oracle	https://ww	A-ORA-					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Hospitality Inventory Management product of Oracle Food and Beverage Applications (component: Export to Reporting and Analytics). The supported version that is affected is 9.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Inventory Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Inventory Management accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). CVE ID : CVE-2021-2311	w.oracle.com/security-alerts/cpuapr2021.html	HOSP-040521/193
http_server					
N/A	22-04-2021	5.8	Vulnerability in the Oracle HTTP Server product of Oracle Fusion Middleware (component: Web Listener). Supported versions that are affected are 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle HTTP Server. Successful attacks require human interaction from a person	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-HTTP-040521/194

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle HTTP Server accessible data as well as unauthorized read access to a subset of Oracle HTTP Server accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N).</p> <p>CVE ID : CVE-2021-2315</p>		

human_resource_management_software_for_france

N/A	22-04-2021	5.5	<p>Vulnerability in the Oracle HRMS (France) product of Oracle E-Business Suite (component: French HR). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle HRMS (France). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle HRMS (France) accessible data as well as unauthorized access to critical data or complete access to all Oracle HRMS (France) accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-HUMA-040521/195
-----	------------	-----	--	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). CVE ID : CVE-2021-2316								
human_resources											
N/A	22-04-2021	5.5	Vulnerability in the Oracle Human Resources product of Oracle E-Business Suite (component: iRecruitment). The supported version that is affected is 12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Human Resources. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Human Resources accessible data as well as unauthorized access to critical data or complete access to all Oracle Human Resources accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). CVE ID : CVE-2021-2260	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-HUMA-040521/196						
hyperion_analytic_provider_services											
N/A	22-04-2021	6.8	Vulnerability in the Hyperion Analytic Provider Services product of Oracle Hyperion (component: JAPI). Supported versions	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-HYPE-040521/197						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that are affected are 11.1.2.4 and 12.2.1.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Hyperion Analytic Provider Services. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Hyperion Analytic Provider Services, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Hyperion Analytic Provider Services. CVSS 3.1 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H). CVE ID : CVE-2021-2244		
hyperion_financial_management					
N/A	22-04-2021	4.6	Vulnerability in the Hyperion Financial Management product of Oracle Hyperion (component: Task Automation). The supported version that is affected is 11.1.2.4. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Hyperion Financial Management. Successful attacks require	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-HYPE-040521/198

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Hyperion Financial Management accessible data as well as unauthorized read access to a subset of Hyperion Financial Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Hyperion Financial Management. CVSS 3.1 Base Score 3.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:L). CVE ID : CVE-2021-2158		
incentive_compensation					
N/A	22-04-2021	5.5	Vulnerability in the Oracle Incentive Compensation product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Incentive Compensation. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-INCE-040521/199

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Oracle Incentive Compensation accessible data as well as unauthorized access to critical data or complete access to all Oracle Incentive Compensation accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).</p> <p>CVE ID : CVE-2021-2228</p>		
installed_base					
N/A	22-04-2021	5.5	<p>Vulnerability in the Oracle Installed Base product of Oracle E-Business Suite (component: APIs). The supported version that is affected is 12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Installed Base. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Installed Base accessible data as well as unauthorized access to critical data or complete access to all Oracle Installed Base accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector:</p>	<p>https://www.oracle.com/security-alerts/cpuapr2021.html</p>	A-ORA-INST-040521/200

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). CVE ID : CVE-2021-2231		
internet_expenses					
N/A	22-04-2021	4.3	Vulnerability in the Oracle Internet Expenses product of Oracle E-Business Suite (component: Mobile Expenses). Supported versions that are affected are 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Internet Expenses. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Internet Expenses accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N). CVE ID : CVE-2021-2153	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-INTE-040521/201
isetup					
N/A	22-04-2021	5.5	Vulnerability in the Oracle iSetup product of Oracle E-Business Suite (component: General Ledger Update Transform, Reports). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-ISET-040521/202

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker with network access via HTTP to compromise Oracle iSetup. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle iSetup accessible data as well as unauthorized access to critical data or complete access to all Oracle iSetup accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).</p> <p>CVE ID : CVE-2021-2276</p>		
istore					
N/A	22-04-2021	5.8	<p>Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this</p>	<p>https://www.oracle.com/security-alerts/cpuapr2021.html</p>	A-ORA-ISTO-040521/203

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). CVE ID : CVE-2021-2182		
N/A	22-04-2021	5.8	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-ISTO-040521/204

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). CVE ID : CVE-2021-2187		
N/A	22-04-2021	5.5	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle iStore. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle iStore accessible data as well as unauthorized access to critical data or complete access to all Oracle iStore accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). CVE ID : CVE-2021-2241	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-ISTO-040521/205
N/A	22-04-2021	5.8	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-ISTO-040521/206

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). CVE ID : CVE-2021-2199		
N/A	22-04-2021	5.8	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-ISTO-040521/207

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). CVE ID : CVE-2021-2183		
N/A	22-04-2021	5.8	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products.	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-ISTO-040521/208

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). CVE ID : CVE-2021-2184		
N/A	22-04-2021	5.8	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-ISTO-040521/209

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
			or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). CVE ID : CVE-2021-2185		
N/A	22-04-2021	5.8	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-ISTO-040521/210

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			/UI:R/S:C/C:H/I:L/A:N). CVE ID : CVE-2021-2186								
N/A	22-04-2021	5.8	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). CVE ID : CVE-2021-2188	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-ISTO-040521/211						
N/A	22-04-2021	5.8	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-ISTO-040521/212						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). CVE ID : CVE-2021-2197	r2021.html	
N/A	22-04-2021	5.8	Vulnerability in the Oracle iStore product of Oracle E-Business Suite (component: Shopping Cart). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore.	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-ISTO-040521/213

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).</p> <p>CVE ID : CVE-2021-2150</p>		
knowledge_management					
N/A	22-04-2021	5.8	<p>Vulnerability in the Oracle Knowledge Management product of Oracle E-Business Suite (component: Setup, Admin). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Knowledge Management. Successful attacks require human interaction from a person other than the attacker and while the</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-KNOW-040521/214

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is in Oracle Knowledge Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Knowledge Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Knowledge Management accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). CVE ID : CVE-2021-2198		
labor_distribution					
N/A	22-04-2021	5.5	Vulnerability in the Oracle Labor Distribution product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Labor Distribution. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Labor Distribution accessible data as well as	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-LABO-040521/215

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>unauthorized access to critical data or complete access to all Oracle Labor Distribution accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).</p> <p>CVE ID : CVE-2021-2267</p>		

landed_cost_management

N/A	22-04-2021	5.5	<p>Vulnerability in the Oracle Landed Cost Management product of Oracle E-Business Suite (component: Shipment Workbench). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Landed Cost Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Landed Cost Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Landed Cost Management accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector:</p>	<p>https://www.oracle.com/security-alerts/cpuapr2021.html</p>	A-ORA-LAND-040521/216
-----	------------	-----	---	--	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			(CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). CVE ID : CVE-2021-2249								
lease_and_finance_management											
N/A	22-04-2021	5.5	Vulnerability in the Oracle Lease and Finance Management product of Oracle E-Business Suite (component: Quotes). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Lease and Finance Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Lease and Finance Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Lease and Finance Management accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). CVE ID : CVE-2021-2261	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-LEAS-040521/217						
loans											
N/A	22-04-2021	5.5	Vulnerability in the Oracle Loans product of Oracle E-Business Suite (component:	https://www.oracle.com/security-	A-ORA-LOAN-040521/218						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Loan Details, Loan Accounting Events). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Loans. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Loans accessible data as well as unauthorized access to critical data or complete access to all Oracle Loans accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).</p> <p>CVE ID : CVE-2021-2252</p>	alerts/cpuap r2021.html	
manufacturing_execution_system_for_process_manufacturing					
N/A	22-04-2021	5.5	<p>Vulnerability in the Oracle MES for Process Manufacturing product of Oracle E-Business Suite (component: Process Operations). The supported version that is affected is 12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle MES for Process Manufacturing. Successful attacks of this vulnerability can result in</p>	https://ww w.oracle.co m/security- alerts/cpuap r2021.html	A-ORA- MANU- 040521/219

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>unauthorized creation, deletion or modification access to critical data or all Oracle MES for Process Manufacturing accessible data as well as unauthorized access to critical data or complete access to all Oracle MES for Process Manufacturing accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).</p> <p>CVE ID : CVE-2021-2238</p>		

marketing

N/A	22-04-2021	6.4	<p>Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Marketing Administration). Supported versions that are affected are 12.2.7-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Marketing accessible data as well as unauthorized access to critical data or complete access to all Oracle Marketing accessible data. CVSS 3.1 Base Score</p>	<p>https://www.oracle.com/security-alerts/cpuapr2021.html</p>	A-ORA-MARK-040521/220
-----	------------	-----	--	--	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N). CVE ID : CVE-2021-2205		
mysql					
N/A	22-04-2021	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2021-2166	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQ-040521/221
N/A	22-04-2021	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQ-040521/222

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2021-2170								
N/A	22-04-2021	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2021-2193	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQL-040521/223						
N/A	22-04-2021	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQL-040521/224						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2021-2196								
N/A	22-04-2021	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2021-2215	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQ-040521/225						
N/A	22-04-2021	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior.	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQ-040521/226						
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						
			Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N). CVE ID : CVE-2021-2226								
N/A	22-04-2021	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2021-2298	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQ-040521/227						
N/A	22-04-2021	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server:	https://www.oracle.com/security-	A-ORA-MYSQ-						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			DML). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2021-2300	alerts/cpuap r2021.html	040521/228
N/A	22-04-2021	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2021-2146	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQL-040521/229

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
N/A	22-04-2021	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.30 and prior and 8.0.17 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2021-2160	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQ-040521/230
N/A	22-04-2021	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Audit Plug-in). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Integrity)	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQ-040521/231

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L /UI:N/S:U/C:N/I:L/A:N). CVE ID : CVE-2021-2162								
N/A	22-04-2021	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H /UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2021-2164	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQ-040521/232						
N/A	22-04-2021	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Partition). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQ-040521/233						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			(complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2021-2201								
N/A	22-04-2021	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.32 and prior and 8.0.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2021-2202	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQL-040521/234						
N/A	22-04-2021	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQL-040521/235						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2021-2203								
N/A	22-04-2021	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Partition). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2021-2208	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQ-040521/236						
N/A	22-04-2021	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQ-040521/237						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2021-2212		
N/A	22-04-2021	5.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). CVE ID : CVE-2021-2304	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQ-040521/238

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	22-04-2021	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2021-2305	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQL-040521/239
N/A	22-04-2021	3.3	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Packaging). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQL-040521/240

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						
			MySQL Server accessible data as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:N). CVE ID : CVE-2021-2307								
N/A	22-04-2021	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N). CVE ID : CVE-2021-2308	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQ-040521/241						
N/A	22-04-2021	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQ-040521/242						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2021-2172								
N/A	22-04-2021	3.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2021-2174	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQL-040521/243						
N/A	22-04-2021	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.32 and prior and	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQL-040521/244						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			8.0.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2021-2178		
N/A	22-04-2021	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2021-2179	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQL-040521/245

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	22-04-2021	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2021-2230	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQL-040521/246
N/A	22-04-2021	1.9	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 8.0.23 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 1.9 (Availability impacts). CVSS	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQL-040521/247

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:L). CVE ID : CVE-2021-2232								
N/A	22-04-2021	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2021-2278	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQ-040521/248						
N/A	22-04-2021	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQ-040521/249						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2021-2293		
N/A	22-04-2021	6.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 5.7.29 and prior and 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H). CVE ID : CVE-2021-2144	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQ-040521/250
N/A	22-04-2021	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQ-040521/251

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2021-2169								
N/A	22-04-2021	3.5	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2021-2171	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQ-040521/252						
N/A	22-04-2021	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQ-040521/253						
CVSS Scoring Scale		0-1	1-2	2-3	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 with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2021-2180								
N/A	22-04-2021	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2021-2194	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQ-040521/254						
N/A	22-04-2021	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQ-040521/255						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2021-2213	r2021.html	
N/A	22-04-2021	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2021-2217	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQL-040521/256

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	22-04-2021	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2021-2299	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQL-040521/257
N/A	22-04-2021	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQL-040521/258

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			/UI:N/S:U/C:L/I:N/A:N). CVE ID : CVE-2021-2301		
N/A	22-04-2021	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 5.7.33 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2021-2154	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-MYSQL-040521/259
one-to-one_fulfillment					
N/A	22-04-2021	4.3	Vulnerability in the Oracle One-to-One Fulfillment product of Oracle E-Business Suite (component: Documents). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker.	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-ONE-040521/260

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N). CVE ID : CVE-2021-2155		
oss_support_tools					
N/A	22-04-2021	4	Vulnerability in the OSS Support Tools product of Oracle Support Tools (component: Diagnostic Assistant). The supported version that is affected is Prior to 2.12.41. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise OSS Support Tools. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all OSS Support Tools accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N). CVE ID : CVE-2021-2303	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-OSS_-040521/261
outside_in_technology					
N/A	22-04-2021	6.4	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component:	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-OUTS-040521/262

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N). CVE ID : CVE-2021-2242	r2021.html	
N/A	22-04-2021	7.5	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion	https://www.oracle.com/security-	A-ORA-OUTS-040521/263

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
			<p>Middleware (component: Outside In Filters). The supported version that is affected is 8.5.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS Base Score depend on the software that uses Outside In Technology. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology, but if data is not received over a network the CVSS score may be lower. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).</p>	alerts/cpuap r2021.html	

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-2240		
partner_management					
N/A	22-04-2021	5.8	<p>Vulnerability in the Oracle Partner Management product of Oracle E-Business Suite (component: Attribute Admin Setup). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Partner Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Partner Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Partner Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Partner Management accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).</p> <p>CVE ID : CVE-2021-2195</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-PART-040521/264

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
payables											
N/A	22-04-2021	5.5	Vulnerability in the Oracle Payables product of Oracle E-Business Suite (component: India Localization, Results). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Payables. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Payables accessible data as well as unauthorized access to critical data or complete access to all Oracle Payables accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). CVE ID : CVE-2021-2259	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-PAYA-040521/265						
peoplesoft_enterprise											
N/A	22-04-2021	6.5	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Security). Supported versions that are affected are 8.56, 8.57 and 8.58. Easily exploitable vulnerability allows high privileged attacker with	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-PEOP-040521/266						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of PeopleSoft Enterprise PeopleTools. CVSS 3.1 Base Score 6.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:H/A:H).</p> <p>CVE ID : CVE-2021-2151</p>		
peoplesoft_enterprise_campus_software_campus_community					
N/A	22-04-2021	3.5	<p>Vulnerability in the PeopleSoft Enterprise CS Campus Community product of Oracle PeopleSoft (component: Frameworks). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise CS Campus Community. Successful attacks require human</p>	<p>https://www.oracle.com/security-alerts/cpuapr2021.html</p>	A-ORA-PEOP-040521/267

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise CS Campus Community accessible data. CVSS 3.1 Base Score 3.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N).</p> <p>CVE ID : CVE-2021-2159</p>		
peoplesoft_enterprise_peopletools					
N/A	22-04-2021	5.8	<p>Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Multichannel Framework). Supported versions that are affected are 8.56, 8.57 and 8.58. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-PEOP-040521/268

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).</p> <p>CVE ID : CVE-2021-2216</p>		
N/A	22-04-2021	6.5	<p>Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: SQR). Supported versions that are affected are 8.56, 8.57 and 8.58. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. While the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-PEOP-040521/269

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PeopleSoft Enterprise PeopleTools. CVSS 3.1 Base Score 7.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L). CVE ID : CVE-2021-2219		
peoplesoft_enterprise_pt_peopletools					
N/A	22-04-2021	7.5	Vulnerability in the PeopleSoft Enterprise PT PeopleTools product of Oracle PeopleSoft (component: Health Center). Supported versions that are affected are 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PT PeopleTools. While the vulnerability is in PeopleSoft Enterprise PT PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PT PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PT PeopleTools accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of PeopleSoft Enterprise PT PeopleTools. CVSS 3.1 Base	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-PEOP-040521/270

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L). CVE ID : CVE-2021-2218							
peoplesoft_enterprise_scm_eprocurement										
N/A	22-04-2021	5.5	Vulnerability in the PeopleSoft Enterprise SCM eProcurement product of Oracle PeopleSoft (component: Manage Requisition Status). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise SCM eProcurement. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise SCM eProcurement accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise SCM eProcurement accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N). CVE ID : CVE-2021-2220	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-PEOP-040521/271					
platform_security_for_java										
N/A	22-04-2021	7.5	Vulnerability in the Oracle	https://ww	A-ORA-					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Platform Security for Java product of Oracle Fusion Middleware (component: OPSS). Supported versions that are affected are 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Platform Security for Java. Successful attacks of this vulnerability can result in takeover of Oracle Platform Security for Java. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). CVE ID : CVE-2021-2302	w.oracle.com/security-alerts/cpuapr2021.html	PLAT-040521/272

product_hub

N/A	22-04-2021	5.5	Vulnerability in the Oracle Product Hub product of Oracle E-Business Suite (component: Template, GTIN search). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Product Hub. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Product Hub	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-PROD-040521/273
-----	------------	-----	---	--	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			accessible data as well as unauthorized access to critical data or complete access to all Oracle Product Hub accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). CVE ID : CVE-2021-2289								
project_contracts											
N/A	22-04-2021	5.5	Vulnerability in the Oracle Project Contracts product of Oracle E-Business Suite (component: Hold Management). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Project Contracts. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Project Contracts accessible data as well as unauthorized access to critical data or complete access to all Oracle Project Contracts accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-PROJ-040521/274						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-2254		
projects					
N/A	22-04-2021	5.5	<p>Vulnerability in the Oracle Projects product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Projects. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Projects accessible data as well as unauthorized access to critical data or complete access to all Oracle Projects accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).</p> <p>CVE ID : CVE-2021-2258</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-PROJ-040521/275
purchasing					
N/A	22-04-2021	5.5	<p>Vulnerability in the Oracle Purchasing product of Oracle E-Business Suite (component: Endeca). The supported version that is affected is 12.1.3. Easily exploitable vulnerability allows low privileged</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-PURC-040521/276

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker with network access via HTTPS to compromise Oracle Purchasing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Purchasing accessible data as well as unauthorized access to critical data or complete access to all Oracle Purchasing accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).</p> <p>CVE ID : CVE-2021-2262</p>		

quoting

N/A	22-04-2021	5.5	<p>Vulnerability in the Oracle Quoting product of Oracle E-Business Suite (component: Courseware). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Quoting. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Quoting accessible data as well as unauthorized access to critical data or complete</p>	<p>https://www.oracle.com/security-alerts/cpuapr2021.html</p>	A-ORA-QUOT-040521/277
-----	------------	-----	--	--	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			access to all Oracle Quoting accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). CVE ID : CVE-2021-2268							
receivables										
N/A	22-04-2021	5.5	Vulnerability in the Oracle Receivables product of Oracle E-Business Suite (component: Receipts). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Receivables. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Receivables accessible data as well as unauthorized access to critical data or complete access to all Oracle Receivables accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). CVE ID : CVE-2021-2223	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-RECE-040521/278					
sales_offline										
N/A	22-04-2021	5	Vulnerability in the Oracle	https://ww	A-ORA-					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Sales Offline product of Oracle E-Business Suite (component: Template). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Sales Offline. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Sales Offline. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).</p> <p>CVE ID : CVE-2021-2189</p>	w.oracle.com/security-alerts/cpuapr2021.html	SALE-040521/279
N/A	22-04-2021	5	<p>Vulnerability in the Oracle Sales Offline product of Oracle E-Business Suite (component: Template). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Sales Offline. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Sales Offline. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-SALE-040521/280

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2021-2190		
secure_global_desktop					
N/A	22-04-2021	7.5	Vulnerability in the Oracle Secure Global Desktop product of Oracle Virtualization (component: Gateway). The supported version that is affected is 5.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Secure Global Desktop. While the vulnerability is in Oracle Secure Global Desktop, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Secure Global Desktop. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H). CVE ID : CVE-2021-2177	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-SECU-040521/281
N/A	22-04-2021	7.5	Vulnerability in the Oracle Secure Global Desktop product of Oracle Virtualization (component: Server). The supported version that is affected is 5.6. Easily exploitable vulnerability allows unauthenticated attacker	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-SECU-040521/282

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>with network access via SKID to compromise Oracle Secure Global Desktop. While the vulnerability is in Oracle Secure Global Desktop, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Secure Global Desktop. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).</p> <p>CVE ID : CVE-2021-2248</p>		
N/A	22-04-2021	6.8	<p>Vulnerability in the Oracle Secure Global Desktop product of Oracle Virtualization (component: Client). The supported version that is affected is 5.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via TLS to compromise Oracle Secure Global Desktop. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Secure Global Desktop, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Secure Global Desktop. CVSS 3.1</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-SECU-040521/283

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H). CVE ID : CVE-2021-2221		
service_contracts					
N/A	22-04-2021	5.5	Vulnerability in the Oracle Service Contracts product of Oracle E-Business Suite (component: Authoring). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Service Contracts. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Service Contracts accessible data as well as unauthorized access to critical data or complete access to all Oracle Service Contracts accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). CVE ID : CVE-2021-2255	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-SERV-040521/284
site_hub					
N/A	22-04-2021	5.5	Vulnerability in the Oracle Site Hub product of Oracle E-Business Suite	https://www.oracle.com/security-	A-ORA-SITE-040521/285

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(component: Sites). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Site Hub. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Site Hub accessible data as well as unauthorized access to critical data or complete access to all Oracle Site Hub accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). CVE ID : CVE-2021-2270	alerts/cpuap r2021.html	
sourcing					
N/A	22-04-2021	5.5	Vulnerability in the Oracle Sourcing product of Oracle E-Business Suite (component: Intelligence, RFx). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Sourcing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-SOUR-040521/286

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			critical data or all Oracle Sourcing accessible data as well as unauthorized access to critical data or complete access to all Oracle Sourcing accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). CVE ID : CVE-2021-2263		
storage_cloud_software_appliance					
N/A	22-04-2021	7.5	Vulnerability in the Oracle Storage Cloud Software Appliance product of Oracle Storage Gateway (component: Management Console). The supported version that is affected is Prior to 16.3.1.4.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Storage Cloud Software Appliance. While the vulnerability is in Oracle Storage Cloud Software Appliance, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Storage Cloud Software Appliance. Note: Updating the Oracle Storage Cloud Software Appliance to version 16.3.1.4.2 or later will address these vulnerabilities. Download	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-STOR-040521/287

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>the latest version of Oracle Storage Cloud Software Appliance from https://www.oracle.com/downloads/cloud/oscsa-downloads.html>here. Refer to Document https://support.oracle.com/rstyp=doc&id=2768897.1>2768897.1 for more details. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).</p> <p>CVE ID : CVE-2021-2256</p>		
N/A	22-04-2021	4	<p>Vulnerability in the Oracle Storage Cloud Software Appliance product of Oracle Storage Gateway (component: Management Console). The supported version that is affected is Prior to 16.3.1.4.2. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Storage Cloud Software Appliance. While the vulnerability is in Oracle Storage Cloud Software Appliance, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Storage Cloud Software Appliance accessible data. Note: Updating the Oracle Storage</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-STOR-040521/288

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Cloud Software Appliance to version 16.3.1.4.2 or later will address these vulnerabilities. Download the latest version of Oracle Storage Cloud Software Appliance from https://www.oracle.com/downloads/cloud/oscsa-downloads.html here. Refer to Document https://support.oracle.com/rstyp=doc&id=2768897.1 for more details. CVSS 3.1 Base Score 4.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N).</p> <p>CVE ID : CVE-2021-2257</p>		
subledger_accounting					
N/A	22-04-2021	5.5	<p>Vulnerability in the Oracle Subledger Accounting product of Oracle E-Business Suite (component: Inquiries). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Subledger Accounting. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Subledger Accounting accessible data as well as unauthorized access to critical data or</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-SUBL-040521/289

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
			complete access to all Oracle Subledger Accounting accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). CVE ID : CVE-2021-2272		
time_and_labor					
N/A	22-04-2021	5.5	Vulnerability in the Oracle Time and Labor product of Oracle E-Business Suite (component: Timecard). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Time and Labor. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Time and Labor accessible data as well as unauthorized access to critical data or complete access to all Oracle Time and Labor accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). CVE ID : CVE-2021-2239	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-TIME-040521/290

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
trade_management					
N/A	22-04-2021	5.8	<p>Vulnerability in the Oracle Trade Management product of Oracle E-Business Suite (component: Quotes). Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).</p> <p>CVE ID : CVE-2021-2206</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-TRAD-040521/291
N/A	22-04-2021	5.8	<p>Vulnerability in the Oracle Trade Management product of Oracle E-Business Suite (component: Quotes).</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-TRAD-040521/292

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Supported versions that are affected are 12.1.1-12.1.3 and 12.2.3-12.2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). CVE ID : CVE-2021-2210	r2021.html	
transportation_execution					
N/A	22-04-2021	5.5	Vulnerability in the Oracle Transportation Execution product of Oracle E-Business Suite (component: Install and Upgrade). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-TRAN-040521/293

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Transportation Execution. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Transportation Execution accessible data as well as unauthorized access to critical data or complete access to all Oracle Transportation Execution accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).</p> <p>CVE ID : CVE-2021-2235</p>		
universal_work_queue					
N/A	22-04-2021	5.5	<p>Vulnerability in the Oracle Universal Work Queue product of Oracle E-Business Suite (component: Work Provider Site Level Administration). Supported versions that are affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Universal Work Queue. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-UNIV-040521/294

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			access to critical data or all Oracle Universal Work Queue accessible data as well as unauthorized access to critical data or complete access to all Oracle Universal Work Queue accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). CVE ID : CVE-2021-2246								
vm_virtualbox											
N/A	22-04-2021	4.4	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-VM_V-040521/295						
CVSS Scoring Scale		0-1	1-2	2-3	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-2021-2309		
N/A	22-04-2021	1.9	<p>Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N).</p> <p>CVE ID : CVE-2021-2296</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-VM_V-040521/296
N/A	22-04-2021	2.1	<p>Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-VM_V-040521/297

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).</p> <p>CVE ID : CVE-2021-2285</p>		
N/A	22-04-2021	2.1	<p>Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 7.1</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-VM_V-040521/298

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			(Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N /UI:N/S:C/C:H/I:N/A:N). CVE ID : CVE-2021-2283								
N/A	22-04-2021	2.1	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H /UI:N/S:C/C:H/I:N/A:N). CVE ID : CVE-2021-2266	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-VM_V-040521/299						
N/A	22-04-2021	2.1	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-VM_V-040521/300						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).</p> <p>CVE ID : CVE-2021-2282</p>		
N/A	22-04-2021	2.1	<p>Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation,</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-VM_V-040521/301

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			deletion or modification access to critical data or all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 7.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:N). CVE ID : CVE-2021-2281								
N/A	22-04-2021	2.1	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N). CVE ID : CVE-2021-2280	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-VM_V-040521/302						
N/A	22-04-2021	6.8	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-VM_V-040521/303						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			supported version that is affected is Prior to 6.1.20. Difficult to exploit vulnerability allows unauthenticated attacker with network access via RDP to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H). CVE ID : CVE-2021-2279	r2021.html	
N/A	22-04-2021	2.1	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 7.1	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-VM_V-040521/304

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N). CVE ID : CVE-2021-2287		
N/A	22-04-2021	4.4	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H). CVE ID : CVE-2021-2145	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-VM_V-040521/305
N/A	22-04-2021	4.6	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-VM_V-040521/306

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
			<p>where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).</p> <p>CVE ID : CVE-2021-2250</p>		
N/A	22-04-2021	4.4	<p>Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector:</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-VM_V-040521/307

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			(CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H). CVE ID : CVE-2021-2310								
N/A	22-04-2021	2.1	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. Note: This vulnerability applies to Windows systems only. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). CVE ID : CVE-2021-2312	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-VM_V-040521/308						
N/A	22-04-2021	1.9	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-VM_V-040521/309						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N).</p> <p>CVE ID : CVE-2021-2297</p>		
N/A	22-04-2021	1.9	<p>Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 4.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N).</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-VM_V-040521/310

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
			CVE ID : CVE-2021-2291		
N/A	22-04-2021	2.1	<p>Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 7.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:N).</p> <p>CVE ID : CVE-2021-2286</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-VM_V-040521/311
N/A	22-04-2021	2.1	<p>Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-VM_V-040521/312

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 7.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:N).</p> <p>CVE ID : CVE-2021-2284</p>		
N/A	22-04-2021	3.6	<p>Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle VM VirtualBox accessible data as well as</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-VM_V-040521/313

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 8.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N).</p> <p>CVE ID : CVE-2021-2264</p>		
N/A	22-04-2021	2.1	<p>Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).</p> <p>CVE ID : CVE-2021-2306</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-VM_V-040521/314
weblogic_server					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	22-04-2021	6.4	<p>Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 6.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L).</p> <p>CVE ID : CVE-2021-2294</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-WEBL-040521/315
N/A	22-04-2021	4.3	<p>Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported versions that are affected are 10.3.6.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-WEBL-040521/316

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). CVE ID : CVE-2021-2211		
N/A	22-04-2021	7.5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Coherence Container). Supported versions that are affected are 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). CVE ID : CVE-2021-2135	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-WEBL-040521/317
N/A	22-04-2021	5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0,	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-WEBL-040521/318

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). CVE ID : CVE-2021-2204		
N/A	22-04-2021	5	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: TopLink Integration). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-WEBL-040521/319

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-2157		
N/A	22-04-2021	3.5	<p>Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 4.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N).</p> <p>CVE ID : CVE-2021-2214</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-WEBL-040521/320
N/A	22-04-2021	5.8	<p>Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). The supported version that is affected is 10.3.6.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-WEBL-040521/321

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).</p> <p>CVE ID : CVE-2021-2142</p>		
N/A	22-04-2021	7.5	<p>Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).</p> <p>CVE ID : CVE-2021-2136</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-WEBL-040521/322

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
work_in_progress					
N/A	22-04-2021	5.5	<p>Vulnerability in the Oracle Work in Process product of Oracle E-Business Suite (component: Resource Exceptions). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Work in Process. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Work in Process accessible data as well as unauthorized access to critical data or complete access to all Oracle Work in Process accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).</p> <p>CVE ID : CVE-2021-2271</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	A-ORA-WORK-040521/323
paloaltonetworks					
bridgecrew_checkov					
Deserialization of Untrusted Data	20-04-2021	6.5	<p>An unsafe deserialization vulnerability in Bridgecrew Checkov by Prisma Cloud allows arbitrary code execution when processing a malicious terraform file. This issue impacts Checkov 2.0 versions earlier than</p>	https://security.paloaltonetworks.com/CVE-2021-3035	A-PAL-BRID-040521/324

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			Checkov 2.0.26. Checkov 1.0 versions are not impacted. CVE ID : CVE-2021-3035								
globalprotect											
Improper Input Validation	20-04-2021	4.9	A denial-of-service (DoS) vulnerability in Palo Alto Networks GlobalProtect app on Windows systems allows a limited Windows user to send specifically-crafted input to the GlobalProtect app that results in a Windows blue screen of death (BSOD) error. This issue impacts: GlobalProtect app 5.1 versions earlier than GlobalProtect app 5.1.8; GlobalProtect app 5.2 versions earlier than GlobalProtect app 5.2.4. CVE ID : CVE-2021-3038	https://security.paloaltonetworks.com/CVE-2021-3038	A-PAL-GLOB-040521/325						
parallels											
parallels_desktop											
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-04-2021	4.6	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 16.1.1-49141. An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the Toolgate component. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to escalate	https://kb.parallels.com/en/125013	A-PAR-PARA-040521/326						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges and execute code in the context of the current user on the host system. Was ZDI-CAN-12130. CVE ID : CVE-2021-27278		
pfsense					
pfsense					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-04-2021	4.3	pfSense 2.5.0 allows XSS via the services_wol_edit.php Description field. CVE ID : CVE-2021-27933	N/A	A-PFS-PFSE-040521/327
php					
php					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-04-2021	4.3	XMB is vulnerable to cross-site scripting (XSS) due to inadequate filtering of BBCode input. This bug affects all versions of XMB. All XMB installations must be updated to versions 1.9.12.03 or 1.9.11.16. CVE ID : CVE-2021-29399	https://www.xmbforum2.com/ , https://docs.xmbforum2.com/index.php?title=Security_Issue_History , https://forums.xmbforum2.com/viewthread.php?tid=777105	A-PHP-PHP-040521/328
picotts_project					
picotts					
Improper Neutralization of Special Elements used in a Command ('Command	18-04-2021	7.5	This affects all versions of package picotts. If attacker-controlled user input is given to the say function, it is possible for an attacker to execute arbitrary commands. This is due to	N/A	A-PIC-PICO-040521/329

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			use of the child_process exec function without input sanitization. CVE ID : CVE-2021-23378		
portkiller_project					
portkiller					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-04-2021	7.5	This affects all versions of package portkiller. If (attacker-controlled) user input is given, it is possible for an attacker to execute arbitrary commands. This is due to use of the child_process exec function without input sanitization. CVE ID : CVE-2021-23379	N/A	A-POR-PORT-040521/330
ps-visitor_project					
ps-visitor					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-04-2021	7.5	This affects all versions of package ps-visitor. If attacker-controlled user input is given to the kill function, it is possible for an attacker to execute arbitrary commands. This is due to use of the child_process exec function without input sanitization. CVE ID : CVE-2021-23374	N/A	A-PS--PS-V-040521/331
psnode_project					
psnode					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-04-2021	7.5	This affects all versions of package psnode. If attacker-controlled user input is given to the kill function, it is possible for an attacker to execute arbitrary commands. This is due to use of the child_process exec function without input	N/A	A-PSN-PSNO-040521/332

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sanitization. CVE ID : CVE-2021-23375		
pulsesecure					
pulse_connect_secure					
Improper Authentication	23-04-2021	7.5	Pulse Connect Secure 9.0R3/9.1R1 and higher is vulnerable to an authentication bypass vulnerability exposed by the Windows File Share Browser and Pulse Secure Collaboration features of Pulse Connect Secure that can allow an unauthenticated user to perform remote arbitrary code execution on the Pulse Connect Secure gateway. This vulnerability has been exploited in the wild. CVE ID : CVE-2021-22893	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44784/ , https://blog.pulsesecure.net/pulse-connect-secure-security-update/	A-PUL-PULS-040521/333
pupnp_project					
pupnp					
Improper Input Validation	20-04-2021	7.5	The Portable SDK for UPnP Devices is an SDK for development of UPnP device and control point applications. The server part of pupnp (libupnp) appears to be vulnerable to DNS rebinding attacks because it does not check the value of the 'Host' header. This can be mitigated by using DNS revolvers which block DNS-rebinding attacks. The vulnerability is fixed in version 1.14.6 and later. CVE ID : CVE-2021-29462	https://github.com/pupnp/pupnp/security/advisories/GHSA-6hqq-w3jq-9fhg	A-PUP-PUPN-040521/334

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
purethemes					
findeo					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2021	4.3	The Realteo WordPress plugin before 1.2.4, used by the Findeo Theme, did not properly sanitise the keyword_search, search_radius._bedrooms and _bathrooms GET parameters before outputting them in its properties page, leading to an unauthenticated reflected Cross-Site Scripting issue. CVE ID : CVE-2021-24237	https://wpscan.com/vulnerability/087b27c4-289e-410f-af74-828a608a4e1e , https://www.docs.purethemes.net/findeo/knowledge-base/change-log-findeo/	A-PUR-FIND-040521/335
Improper Access Control	22-04-2021	4	The Realteo WordPress plugin before 1.2.4, used by the Findeo Theme, did not ensure that the requested property to be deleted belong to the user making the request, allowing any authenticated users to delete arbitrary properties by tampering with the property_id parameter. CVE ID : CVE-2021-24238	https://wpscan.com/vulnerability/b8434eb2-f522-484f-9227-5f581e7f48a5 , https://www.docs.purethemes.net/findeo/knowledge-base/change-log-findeo/	A-PUR-FIND-040521/336
realteo					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2021	4.3	The Realteo WordPress plugin before 1.2.4, used by the Findeo Theme, did not properly sanitise the keyword_search, search_radius._bedrooms and _bathrooms GET parameters before outputting them in its	https://wpscan.com/vulnerability/087b27c4-289e-410f-af74-828a608a4e1e , https://www	A-PUR-REAL-040521/337

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			properties page, leading to an unauthenticated reflected Cross-Site Scripting issue. CVE ID : CVE-2021-24237	w.docs.purethememes.net/findeo/knowledge-base/change-log-findeo/	
Improper Access Control	22-04-2021	4	The Realteo WordPress plugin before 1.2.4, used by the Findeo Theme, did not ensure that the requested property to be deleted belong to the user making the request, allowing any authenticated users to delete arbitrary properties by tampering with the property_id parameter. CVE ID : CVE-2021-24238	https://wpSCAN.com/vulnerability/b8434eb2-f522-484f-9227-5f581e7f48a5, https://www.docs.purethememes.net/findeo/knowledge-base/change-log-findeo/	A-PUR-REAL-040521/338
purl_project					
purl					
N/A	23-04-2021	7.5	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in purl 2.3.2 allows a malicious user to inject properties into Object.prototype. CVE ID : CVE-2021-20089	N/A	A-PUR-PURL-040521/339
remoteclinic					
remote_clinic					
Improper Neutralization of Input During Web Page Generation ('Cross-site	21-04-2021	3.5	Cross Site Scripting (XSS) in Remote Clinic v2.0 via the "Chat" and "Personal Address" field on staff/register.php CVE ID : CVE-2021-31329	N/A	A-REM-REMO-040521/340

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						
Scripting')											
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-04-2021	3.5	Stored XSS in Remote Clinic v2.0 in /medicines due to Medicine Name Field. CVE ID : CVE-2021-31327	N/A	A-REM-REMO-040521/341						
roar-pidusage_project											
roar-pidusage											
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-04-2021	7.5	This affects all versions of package roar-pidusage. If attacker-controlled user input is given to the stat function of this package on certain operating systems, it is possible for an attacker to execute arbitrary commands. This is due to use of the child_process exec function without input sanitization. CVE ID : CVE-2021-23380	N/A	A-ROA-ROAR-040521/342						
rpm_spec_project											
rpm_spec											
N/A	16-04-2021	7.5	The unofficial vscode-rpm-spec extension before 0.3.2 for Visual Studio Code allows remote code execution via a crafted workspace configuration. CVE ID : CVE-2021-31414	https://github.com/LaurentTreguier/vscode-rpm-spec/commit/e19fb8e29cb48cadfd3238371e060d4ffd3384f9	A-RPM-RPM_-040521/343						
ruby-lang											
rexml											
Improper Restriction of XML External	21-04-2021	5	The REXML gem before 3.2.5 in Ruby before 2.6.7, 2.7.x before 2.7.3, and 3.x	https://www.ruby-lang.org/en/	A-RUB-REXM-040521/344						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Entity Reference			before 3.0.1 does not properly address XML round-trip issues. An incorrect document can be produced after parsing and serializing. CVE ID : CVE-2021-28965	news/2021/04/05/xml-round-trip-vulnerability-in-rexml-cve-2021-28965/	
ruby					
Improper Restriction of XML External Entity Reference	21-04-2021	5	The REXML gem before 3.2.5 in Ruby before 2.6.7, 2.7.x before 2.7.3, and 3.x before 3.0.1 does not properly address XML round-trip issues. An incorrect document can be produced after parsing and serializing. CVE ID : CVE-2021-28965	https://www.ruby-lang.org/en/news/2021/04/05/xml-round-trip-vulnerability-in-rexml-cve-2021-28965/	A-RUB-RUBY-040521/345
samba					
cifs-utils					
Incorrect Privilege Assignment	19-04-2021	4.9	A flaw was found in cifs-utils in versions before 6.13. A user when mounting a krb5 CIFS file system from within a container can use Kerberos credentials of the host. The highest threat from this vulnerability is to data confidentiality and integrity. CVE ID : CVE-2021-20208	https://bugzilla.samba.org/show_bug.cgi?id=14651	A-SAM-CIFS-040521/346
siemens					
nucleus_4					
Use of Insufficiently Random Values	22-04-2021	5	A vulnerability has been identified in Nucleus 4 (All versions < V4.1.0), Nucleus NET (All versions), Nucleus RTOS (versions including affected DNS modules), Nucleus ReadyStart (All	https://certportal.siemens.com/productcert/pdf/ssa-705111.pdf , https://cert-	A-SIE-NUCL-040521/347

CVSS Scoring Scale	0-1	1-2	2-3	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 < V2017.02.3), Nucleus Source Code (versions including affected DNS modules), SIMOTICS CONNECT 400 (All versions < V0.5.0.0), SIMOTICS CONNECT 400 (All versions >= V0.5.0.0), VSTAR (versions including affected DNS modules). The DNS client does not properly randomize DNS transaction IDs. That could allow an attacker to poison the DNS cache or spoof DNS resolving. CVE ID : CVE-2021-25677	portal.siemens.com/productcert/pdf/ssa-669158.pdf							
Loop with Unreachable Exit Condition ('Infinite Loop')	22-04-2021	5	A vulnerability has been identified in Nucleus 4 (All versions < V4.1.0), Nucleus NET (All versions), Nucleus ReadyStart (All versions), Nucleus Source Code (versions including affected IPv6 stack), VSTAR (versions including affected IPv6 stack). The function that processes IPv6 headers does not check the lengths of extension header options, allowing attackers to put this function into an infinite loop with crafted length values. CVE ID : CVE-2021-25663	https://cert-portal.siemens.com/productcert/pdf/ssa-248289.pdf, https://us-cert.cisa.gov/ics/advisories/icsa-21-103-05	A-SIE-NUCL-040521/348						
Loop with Unreachable Exit Condition ('Infinite Loop')	22-04-2021	5	A vulnerability has been identified in Nucleus 4 (All versions < V4.1.0), Nucleus NET (All versions), Nucleus ReadyStart (All versions), Nucleus Source Code (versions including affected IPv6 stack), VSTAR	https://cert-portal.siemens.com/productcert/pdf/ssa-248289.pdf	A-SIE-NUCL-040521/349						
CVSS Scoring Scale		0-1	1-2	2-3	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 including affected IPv6 stack). The function that processes the Hop-by-Hop extension header in IPv6 packets and its options lacks any checks against the length field of the header, allowing attackers to put the function into an infinite loop by supplying arbitrary length values. CVE ID : CVE-2021-25664		
nucleus_net					
Use of Insufficiently Random Values	22-04-2021	5	A vulnerability has been identified in Nucleus 4 (All versions < V4.1.0), Nucleus NET (All versions), Nucleus RTOS (versions including affected DNS modules), Nucleus ReadyStart (All versions < V2017.02.3), Nucleus Source Code (versions including affected DNS modules), SIMOTICS CONNECT 400 (All versions < V0.5.0.0), SIMOTICS CONNECT 400 (All versions >= V0.5.0.0), VSTAR (versions including affected DNS modules). The DNS client does not properly randomize DNS transaction IDs. That could allow an attacker to poison the DNS cache or spoof DNS resolving. CVE ID : CVE-2021-25677	https://certportal.siemens.com/productcert/pdf/ssa-705111.pdf , https://certportal.siemens.com/productcert/pdf/ssa-669158.pdf	A-SIE-NUCL-040521/350
Loop with Unreachable Exit Condition ('Infinite	22-04-2021	5	A vulnerability has been identified in Nucleus 4 (All versions < V4.1.0), Nucleus NET (All versions), Nucleus ReadyStart (All versions),	https://certportal.siemens.com/productcert/pdf/ssa-	A-SIE-NUCL-040521/351

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Loop')			Nucleus Source Code (versions including affected IPv6 stack), VSTAR (versions including affected IPv6 stack). The function that processes IPv6 headers does not check the lengths of extension header options, allowing attackers to put this function into an infinite loop with crafted length values. CVE ID : CVE-2021-25663	248289.pdf, https://us-cert.cisa.gov/ics/advisories/icsa-21-103-05	
Loop with Unreachable Exit Condition ('Infinite Loop')	22-04-2021	5	A vulnerability has been identified in Nucleus 4 (All versions < V4.1.0), Nucleus NET (All versions), Nucleus ReadyStart (All versions), Nucleus Source Code (versions including affected IPv6 stack), VSTAR (versions including affected IPv6 stack). The function that processes the Hop-by-Hop extension header in IPv6 packets and its options lacks any checks against the length field of the header, allowing attackers to put the function into an infinite loop by supplying arbitrary length values. CVE ID : CVE-2021-25664	https://certportal.siemens.com/productcert/pdf/ssa-248289.pdf	A-SIE-NUCL-040521/352
Use of Insufficiently Random Values	22-04-2021	5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus RTOS (versions including affected DNS modules), Nucleus ReadyStart (All versions < V2013.08), Nucleus Source Code (versions including affected DNS modules), VSTAR	https://certportal.siemens.com/productcert/pdf/ssa-201384.pdf	A-SIE-NUCL-040521/353

CVSS Scoring Scale	0-1	1-2	2-3	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 including affected DNS modules). The DNS client does not properly randomize UDP port numbers of DNS requests. That could allow an attacker to poison the DNS cache or spoof DNS resolving. CVE ID : CVE-2021-27393		
nucleus_readystart					
Use of Insufficiently Random Values	22-04-2021	5	A vulnerability has been identified in Nucleus 4 (All versions < V4.1.0), Nucleus NET (All versions), Nucleus RTOS (versions including affected DNS modules), Nucleus ReadyStart (All versions < V2017.02.3), Nucleus Source Code (versions including affected DNS modules), SIMOTICS CONNECT 400 (All versions < V0.5.0.0), SIMOTICS CONNECT 400 (All versions >= V0.5.0.0), VSTAR (versions including affected DNS modules). The DNS client does not properly randomize DNS transaction IDs. That could allow an attacker to poison the DNS cache or spoof DNS resolving. CVE ID : CVE-2021-25677	https://cert-portal.siemens.com/productcert/pdf/ssa-705111.pdf , https://cert-portal.siemens.com/productcert/pdf/ssa-669158.pdf	A-SIE-NUCL-040521/354
Loop with Unreachable Exit Condition ('Infinite Loop')	22-04-2021	5	A vulnerability has been identified in Nucleus 4 (All versions < V4.1.0), Nucleus NET (All versions), Nucleus ReadyStart (All versions), Nucleus Source Code (versions including affected	https://cert-portal.siemens.com/productcert/pdf/ssa-248289.pdf , https://us-	A-SIE-NUCL-040521/355

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPv6 stack), VSTAR (versions including affected IPv6 stack). The function that processes IPv6 headers does not check the lengths of extension header options, allowing attackers to put this function into an infinite loop with crafted length values. CVE ID : CVE-2021-25663	cert.cisa.gov/ics/advisories/icsa-21-103-05	
Loop with Unreachable Exit Condition ('Infinite Loop')	22-04-2021	5	A vulnerability has been identified in Nucleus 4 (All versions < V4.1.0), Nucleus NET (All versions), Nucleus ReadyStart (All versions), Nucleus Source Code (versions including affected IPv6 stack), VSTAR (versions including affected IPv6 stack). The function that processes the Hop-by-Hop extension header in IPv6 packets and its options lacks any checks against the length field of the header, allowing attackers to put the function into an infinite loop by supplying arbitrary length values. CVE ID : CVE-2021-25664	https://certportal.siemens.com/productcert/pdf/ssa-248289.pdf	A-SIE-NUCL-040521/356
Use of Insufficiently Random Values	22-04-2021	5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus RTOS (versions including affected DNS modules), Nucleus ReadyStart (All versions < V2013.08), Nucleus Source Code (versions including affected DNS modules), VSTAR (versions including affected DNS modules). The DNS	https://certportal.siemens.com/productcert/pdf/ssa-201384.pdf	A-SIE-NUCL-040521/357

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			client does not properly randomize UDP port numbers of DNS requests. That could allow an attacker to poison the DNS cache or spoof DNS resolving. CVE ID : CVE-2021-27393		
nucleus_source_code					
Use of Insufficiently Random Values	22-04-2021	5	A vulnerability has been identified in Nucleus 4 (All versions < V4.1.0), Nucleus NET (All versions), Nucleus RTOS (versions including affected DNS modules), Nucleus ReadyStart (All versions < V2017.02.3), Nucleus Source Code (versions including affected DNS modules), SIMOTICS CONNECT 400 (All versions < V0.5.0.0), SIMOTICS CONNECT 400 (All versions >= V0.5.0.0), VSTAR (versions including affected DNS modules). The DNS client does not properly randomize DNS transaction IDs. That could allow an attacker to poison the DNS cache or spoof DNS resolving. CVE ID : CVE-2021-25677	https://certportal.siemens.com/productcert/pdf/ssa-705111.pdf , https://certportal.siemens.com/productcert/pdf/ssa-669158.pdf	A-SIE-NUCL-040521/358
Loop with Unreachable Exit Condition ('Infinite Loop')	22-04-2021	5	A vulnerability has been identified in Nucleus 4 (All versions < V4.1.0), Nucleus NET (All versions), Nucleus ReadyStart (All versions), Nucleus Source Code (versions including affected IPv6 stack), VSTAR (versions including affected	https://certportal.siemens.com/productcert/pdf/ssa-248289.pdf , https://us-cert.cisa.gov/ics/advisor	A-SIE-NUCL-040521/359

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPv6 stack). The function that processes IPv6 headers does not check the lengths of extension header options, allowing attackers to put this function into an infinite loop with crafted length values. CVE ID : CVE-2021-25663	ies/icsa-21-103-05	
Loop with Unreachable Exit Condition ('Infinite Loop')	22-04-2021	5	A vulnerability has been identified in Nucleus 4 (All versions < V4.1.0), Nucleus NET (All versions), Nucleus ReadyStart (All versions), Nucleus Source Code (versions including affected IPv6 stack), VSTAR (versions including affected IPv6 stack). The function that processes the Hop-by-Hop extension header in IPv6 packets and its options lacks any checks against the length field of the header, allowing attackers to put the function into an infinite loop by supplying arbitrary length values. CVE ID : CVE-2021-25664	https://certportal.siemens.com/productcert/pdf/ssa-248289.pdf	A-SIE-NUCL-040521/360
Use of Insufficiently Random Values	22-04-2021	5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus RTOS (versions including affected DNS modules), Nucleus ReadyStart (All versions < V2013.08), Nucleus Source Code (versions including affected DNS modules), VSTAR (versions including affected DNS modules). The DNS client does not properly randomize UDP port	https://certportal.siemens.com/productcert/pdf/ssa-201384.pdf	A-SIE-NUCL-040521/361

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			numbers of DNS requests. That could allow an attacker to poison the DNS cache or spoof DNS resolving. CVE ID : CVE-2021-27393		
opcenter_quality					
Use of Hard-coded Cryptographic Key	22-04-2021	7.5	A vulnerability has been identified in Opcenter Quality (All versions < V12.2), QMS Automotive (All versions < V12.30). A private sign key is shipped with the product without adequate protection. CVE ID : CVE-2021-27389	https://cert-portal.siemens.com/productcert/pdf/ssa-788287.pdf	A-SIE-OPCE-040521/362
qms_automotive					
Use of Hard-coded Cryptographic Key	22-04-2021	7.5	A vulnerability has been identified in Opcenter Quality (All versions < V12.2), QMS Automotive (All versions < V12.30). A private sign key is shipped with the product without adequate protection. CVE ID : CVE-2021-27389	https://cert-portal.siemens.com/productcert/pdf/ssa-788287.pdf	A-SIE-QMS_-040521/363
siveillance_video_open_network_bridge					
Insufficiently Protected Credentials	22-04-2021	4	A vulnerability has been identified in Siveillance Video Open Network Bridge (2020 R3), Siveillance Video Open Network Bridge (2020 R2), Siveillance Video Open Network Bridge (2020 R1), Siveillance Video Open Network Bridge (2019 R3), Siveillance Video Open Network Bridge (2019 R2), Siveillance Video Open Network Bridge (2019 R1), Siveillance Video	https://cert-portal.siemens.com/productcert/pdf/ssa-853866.pdf	A-SIE-SIVE-040521/364

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Open Network Bridge (2018 R3), Siveillance Video Open Network Bridge (2018 R2). Affected Open Network Bridges store user credentials for the authentication between ONVIF clients and ONVIF server using a hard-coded key. The encrypted credentials can be retrieved via the MIP SDK. This could allow an authenticated remote attacker to retrieve and decrypt all credentials stored on the ONVIF server.</p> <p>CVE ID : CVE-2021-27392</p>		
solid_edge_se2020					
Out-of-bounds Write	22-04-2021	6.8	<p>A vulnerability has been identified in Solid Edge SE2020 (All versions < SE2020MP13), Solid Edge SE2020 (SE2020MP13), Solid Edge SE2021 (All Versions < SE2021MP4). Affected applications lack proper validation of user-supplied data when parsing PAR files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12529)</p> <p>CVE ID : CVE-2021-25678</p>	https://certportal.siemens.com/productcert/pdf/ssa-574442.pdf	A-SIE-SOLI-040521/365
Out-of-bounds Write	22-04-2021	6.8	<p>A vulnerability has been identified in Solid Edge SE2020 (All versions < SE2020MP13), Solid Edge SE2020 (SE2020MP13),</p>	https://certportal.siemens.com/productcert/pdf/ssa-	A-SIE-SOLI-040521/366

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Solid Edge SE2021 (All Versions < SE2021MP4). Affected applications lack proper validation of user-supplied data when parsing of PAR files. This could result in a stack based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13040) CVE ID : CVE-2021-27382	574442.pdf, https://us-cert.cisa.gov/ics/advisories/icsa-21-103-06	
solid_edge_se2021					
Out-of-bounds Write	22-04-2021	6.8	A vulnerability has been identified in Solid Edge SE2020 (All versions < SE2020MP13), Solid Edge SE2020 (SE2020MP13), Solid Edge SE2021 (All Versions < SE2021MP4). Affected applications lack proper validation of user-supplied data when parsing PAR files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12529) CVE ID : CVE-2021-25678	https://certportal.siemens.com/productcert/pdf/ssa-574442.pdf	A-SIE-SOLI-040521/367
Out-of-bounds Write	22-04-2021	6.8	A vulnerability has been identified in Solid Edge SE2020 (All versions < SE2020MP13), Solid Edge SE2020 (SE2020MP13), Solid Edge SE2021 (All Versions < SE2021MP4). Affected applications lack	https://certportal.siemens.com/productcert/pdf/ssa-574442.pdf , https://us-cert.cisa.gov	A-SIE-SOLI-040521/368

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			proper validation of user-supplied data when parsing of PAR files. This could result in a stack based buffer overflow. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13040) CVE ID : CVE-2021-27382	/ics/advisories/icsa-21-103-06	
tecnomatix_robotexpert					
Out-of-bounds Write	22-04-2021	6.8	A vulnerability has been identified in Tecnomatix RobotExpert (All versions < V16.1). Affected applications lack proper validation of user-supplied data when parsing CELL files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12608) CVE ID : CVE-2021-25670	https://cert-portal.siemens.com/productcert/pdf/ssa-163226.pdf	A-SIE-TECN-040521/369
vstar					
Use of Insufficiently Random Values	22-04-2021	5	A vulnerability has been identified in Nucleus 4 (All versions < V4.1.0), Nucleus NET (All versions), Nucleus RTOS (versions including affected DNS modules), Nucleus ReadyStart (All versions < V2017.02.3), Nucleus Source Code (versions including affected DNS modules), SIMOTICS CONNECT 400 (All versions < V0.5.0.0), SIMOTICS	https://cert-portal.siemens.com/productcert/pdf/ssa-705111.pdf , https://cert-portal.siemens.com/productcert/pdf/ssa-669158.pdf	A-SIE-VSTA-040521/370

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			CONNECT 400 (All versions >= V0.5.0.0), VSTAR (versions including affected DNS modules). The DNS client does not properly randomize DNS transaction IDs. That could allow an attacker to poison the DNS cache or spoof DNS resolving. CVE ID : CVE-2021-25677								
Loop with Unreachable Exit Condition ('Infinite Loop')	22-04-2021	5	A vulnerability has been identified in Nucleus 4 (All versions < V4.1.0), Nucleus NET (All versions), Nucleus ReadyStart (All versions), Nucleus Source Code (versions including affected IPv6 stack), VSTAR (versions including affected IPv6 stack). The function that processes IPv6 headers does not check the lengths of extension header options, allowing attackers to put this function into an infinite loop with crafted length values. CVE ID : CVE-2021-25663	https://cert-portal.siemens.com/productcert/pdf/ssa-248289.pdf , https://us-cert.cisa.gov/ics/advisories/icsa-21-103-05	A-SIE-VSTA-040521/371						
Loop with Unreachable Exit Condition ('Infinite Loop')	22-04-2021	5	A vulnerability has been identified in Nucleus 4 (All versions < V4.1.0), Nucleus NET (All versions), Nucleus ReadyStart (All versions), Nucleus Source Code (versions including affected IPv6 stack), VSTAR (versions including affected IPv6 stack). The function that processes the Hop-by-Hop extension header in IPv6 packets and its options lacks any checks against the	https://cert-portal.siemens.com/productcert/pdf/ssa-248289.pdf	A-SIE-VSTA-040521/372						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			length field of the header, allowing attackers to put the function into an infinite loop by supplying arbitrary length values. CVE ID : CVE-2021-25664		
Use of Insufficiently Random Values	22-04-2021	5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus RTOS (versions including affected DNS modules), Nucleus ReadyStart (All versions < V2013.08), Nucleus Source Code (versions including affected DNS modules), VSTAR (versions including affected DNS modules). The DNS client does not properly randomize UDP port numbers of DNS requests. That could allow an attacker to poison the DNS cache or spoof DNS resolving. CVE ID : CVE-2021-27393	https://certportal.siemens.com/productcert/pdf/ssa-201384.pdf	A-SIE-VSTA-040521/373
solarwinds					
orion_virtual_infrastructure_monitor					
Deserialization of Untrusted Data	22-04-2021	7.2	This vulnerability allows local attackers to escalate privileges on affected installations of SolarWinds Orion Virtual Infrastructure Monitor 2020.2. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the OneTimeJobSchedulerEventsService WCF service. The	https://documentation.solarwinds.com/en/Success_Center/SAM/Content/Release_Notes/SAM_2020-2-5_release_notes.htm#Fixed	A-SOL-ORIO-040521/374

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-11955. CVE ID : CVE-2021-27277		
sonicwall					
email_security					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-04-2021	4	SonicWall Email Security version 10.0.9.x contains a vulnerability that allows a post-authenticated attacker to read an arbitrary file on the remote host. CVE ID : CVE-2021-20023	https://psirt.global.sonicwall.com/vuln-detail/SNWL-ID-2021-0010	A-SON-EMAI-040521/375
telegram					
telegram					
N/A	20-04-2021	3.5	The Telegram app 7.6.2 for iOS allows remote authenticated users to cause a denial of service (application crash) if the victim pastes an attacker-supplied message (e.g., in the Persian language) into a channel or group. The crash occurs in MtProtoKitFramework. CVE ID : CVE-2021-30496	https://t.me/joinchat/bJ9cnUosVh03ZTI0	A-TEL-TELE-040521/376
themeum					
tutor_lms					
Improper Limitation of	22-04-2021	5.5	The Tutor LMS “eLearning and online	https://wpscan.com/vul	A-THE-TUTO-

CVSS Scoring Scale	0-1	1-2	2-3	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 Pathname to a Restricted Directory ('Path Traversal')			course solution WordPress plugin before 1.8.8 is affected by a local file inclusion vulnerability through the maliciously constructed sub_page parameter of the plugin's Tools, allowing high privilege users to include any local php file CVE ID : CVE-2021-24242	nerability/20f3e63a-31d8-49a0-b4ef-209749feff5c	040521/377						
tibco											
administrator											
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-04-2021	6.8	The Administration GUI component of TIBCO Software Inc.'s TIBCO Administrator - Enterprise Edition, TIBCO Administrator - Enterprise Edition, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric, TIBCO Administrator - Enterprise Edition for z/Linux, TIBCO Administrator - Enterprise Edition for z/Linux, TIBCO Runtime Agent, TIBCO Runtime Agent, TIBCO Runtime Agent for z/Linux, and TIBCO Runtime Agent for z/Linux contains an easily exploitable vulnerability that allows an unauthenticated attacker to social engineer a legitimate user with network access to execute a Stored XSS attack targeting the affected system. A successful attack	http://www.tibco.com/services/support/advisories , https://www.tibco.com/support/advisories/2021/04/tibco-security-advisory-april-20-2021-tibco-administrator-2021-28827	A-TIB-ADMIN-040521/378						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>using this vulnerability requires human interaction from a person other than the attacker. Affected releases are TIBCO Software Inc.'s TIBCO Administrator - Enterprise Edition: versions 5.10.2 and below, TIBCO Administrator - Enterprise Edition: versions 5.11.0 and 5.11.1, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric: versions 5.10.2 and below, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric: versions 5.11.0 and 5.11.1, TIBCO Administrator - Enterprise Edition for z/Linux: versions 5.10.2 and below, TIBCO Administrator - Enterprise Edition for z/Linux: versions 5.11.0 and 5.11.1, TIBCO Runtime Agent: versions 5.10.2 and below, TIBCO Runtime Agent: versions 5.11.0 and 5.11.1, TIBCO Runtime Agent for z/Linux: versions 5.10.2 and below, and TIBCO Runtime Agent for z/Linux: versions 5.11.0 and 5.11.1.</p> <p>CVE ID : CVE-2021-28827</p>		
Improper Neutralization of Special Elements used in an SQL	20-04-2021	6.5	<p>The Administration GUI component of TIBCO Software Inc.'s TIBCO Administrator - Enterprise Edition, TIBCO Administrator - Enterprise</p>	http://www.tibco.com/services/support/advisories , https://www	A-TIB-ADMIN-040521/379

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			<p>Edition, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric, TIBCO Administrator - Enterprise Edition for z/Linux, and TIBCO Administrator - Enterprise Edition for z/Linux contains an easily exploitable vulnerability that allows a low privileged attacker with network access to execute a SQL injection attack on the affected system. Affected releases are TIBCO Software Inc.'s TIBCO Administrator - Enterprise Edition: versions 5.10.2 and below, TIBCO Administrator - Enterprise Edition: versions 5.11.0 and 5.11.1, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric: versions 5.10.2 and below, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric: versions 5.11.0 and 5.11.1, TIBCO Administrator - Enterprise Edition for z/Linux: versions 5.10.2 and below, and TIBCO Administrator - Enterprise Edition for z/Linux: versions 5.11.0 and 5.11.1.</p> <p>CVE ID : CVE-2021-28828</p>	w.tibco.com/support/advisories/2021/04/tibco-security-advisory-april-20-2021-tibco-administrator-2021-28828	
Improper	20-04-2021	6	The Administration GUI	http://www.	A-TIB-ADMI-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')			<p>component of TIBCO Software Inc.'s TIBCO Administrator - Enterprise Edition, TIBCO Administrator - Enterprise Edition, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric, TIBCO Administrator - Enterprise Edition for z/Linux, and TIBCO Administrator - Enterprise Edition for z/Linux contains an easily exploitable vulnerability that allows a low privileged attacker with network access to execute a persistent CSV injection attack from the affected system. A successful attack using this vulnerability requires human interaction from a person other than the attacker. Affected releases are TIBCO Software Inc.'s TIBCO Administrator - Enterprise Edition: versions 5.10.2 and below, TIBCO Administrator - Enterprise Edition: versions 5.11.0 and 5.11.1, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric: versions 5.10.2 and below, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric: versions 5.11.0 and 5.11.1,</p>	<p>tibco.com/services/support/advisories, https://www.tibco.com/support/advisories/2021/04/tibco-security-advisory-april-20-2021-tibco-administrator-2021-28829</p>	040521/380

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			TIBCO Administrator - Enterprise Edition for z/Linux: versions 5.10.2 and below, and TIBCO Administrator - Enterprise Edition for z/Linux: versions 5.11.0 and 5.11.1. CVE ID : CVE-2021-28829		
runtime_agent					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-04-2021	6.8	The Administration GUI component of TIBCO Software Inc.'s TIBCO Administrator - Enterprise Edition, TIBCO Administrator - Enterprise Edition, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric, TIBCO Administrator - Enterprise Edition for z/Linux, TIBCO Administrator - Enterprise Edition for z/Linux, TIBCO Runtime Agent, TIBCO Runtime Agent, TIBCO Runtime Agent for z/Linux, and TIBCO Runtime Agent for z/Linux contains an easily exploitable vulnerability that allows an unauthenticated attacker to social engineer a legitimate user with network access to execute a Stored XSS attack targeting the affected system. A successful attack using this vulnerability requires human interaction from a person other than the attacker. Affected	http://www.tibco.com/services/support/advisories , https://www.tibco.com/support/advisories/2021/04/tibco-security-advisory-april-20-2021-tibco-administrator-2021-28827	A-TIB-RUNT-040521/381

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					
			releases are TIBCO Software Inc.'s TIBCO Administrator - Enterprise Edition: versions 5.10.2 and below, TIBCO Administrator - Enterprise Edition: versions 5.11.0 and 5.11.1, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric: versions 5.10.2 and below, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric: versions 5.11.0 and 5.11.1, TIBCO Administrator - Enterprise Edition for z/Linux: versions 5.10.2 and below, TIBCO Administrator - Enterprise Edition for z/Linux: versions 5.11.0 and 5.11.1, TIBCO Runtime Agent: versions 5.10.2 and below, TIBCO Runtime Agent: versions 5.11.0 and 5.11.1, TIBCO Runtime Agent for z/Linux: versions 5.10.2 and below, and TIBCO Runtime Agent for z/Linux: versions 5.11.0 and 5.11.1. CVE ID : CVE-2021-28827							
torchbox										
wagtail										
Improper Neutralization of Input During Web Page Generation ('Cross-site	19-04-2021	3.5	Wagtail is a Django content management system. In affected versions of Wagtail, when saving the contents of a rich text field in the admin interface, Wagtail does not apply server-side checks to ensure that link URLs use a	https://github.com/wagtail/wagtail/security/advisories/GHSA-A-wq5h-f9p5-q7fx	A-TOR-WAGT-040521/382					
CVSS Scoring Scale	0-1	1-2	2-3	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')			valid protocol. A malicious user with access to the admin interface could thus craft a POST request to publish content with `javascript:` URLs containing arbitrary code. The vulnerability is not exploitable by an ordinary site visitor without access to the Wagtail admin. See referenced GitHub advisory for additional details, including a workaround. Patched versions have been released as Wagtail 2.11.7 (for the LTS 2.11 branch) and Wagtail 2.12.4 (for the current 2.12 branch). CVE ID : CVE-2021-29434		

trendmicro

antivirus

Improper Privilege Management	22-04-2021	4.6	Trend Micro Antivirus for Mac 2020 v10.5 and 2021 v11 (Consumer) is vulnerable to an improper access control privilege escalation vulnerability that could allow an attacker to establish a connection that could lead to full local privilege escalation within the application. Please note that an attacker must first obtain the ability to execute low-privileged code on the target system to exploit this vulnerability. CVE ID : CVE-2021-28648	https://helpcenter.trendmicro.com/en-us/article/TMKA-10293	A-TRE-ANTI-040521/383
-------------------------------	------------	-----	---	---	-----------------------

tribalsystems

zenario

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-04-2021	6.4	SQL Injection in Tribalsystems Zenario CMS 8.8.52729 allows remote attackers to access the database or delete the plugin. This is accomplished via the `ID` input field of ajax.php in the `Pugin library - delete` module. CVE ID : CVE-2021-26830	https://github.com/TribalSystems/Zenario/releases/tag/8.8.53370	A-TRI-ZENA-040521/384						
unisys											
stealth											
N/A	20-04-2021	4	Unisys Stealth (core) 5.x before 5.0.048.0, 5.1.x before 5.1.017.0, and 6.x before 6.0.037.0 stores passwords in a recoverable format. CVE ID : CVE-2021-28492	https://public.support.unisys.com/common/public/vulnerability/NVD_Home.aspx , https://public.support.unisys.com/common/public/vulnerability/NVD_Detail_Rpt.aspx?ID=63	A-UNI-STEAL-040521/385						
vaadin											
flow											
Observable Discrepancy	23-04-2021	1.9	Non-constant-time comparison of CSRF tokens in UIDL request handler in com.vaadin:flow-server versions 1.0.0 through 1.0.13 (Vaadin 10.0.0 through 10.0.16), 1.1.0 prior to 2.0.0 (Vaadin 11 prior to 14), 2.0.0 through 2.4.6 (Vaadin 14.0.0 through 14.4.6), 3.0.0 prior to 5.0.0 (Vaadin 15 prior to 18), and 5.0.0 through 5.0.2	https://vaadin.com/security/cve-2021-31404 , https://github.com/vaadin/flow/pull/9875	A-VAA-FLOW-040521/386						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			(Vaadin 18.0.0 through 18.0.5) allows attacker to guess a security token via timing attack. CVE ID : CVE-2021-31404								
Observable Discrepancy	23-04-2021	1.9	Non-constant-time comparison of CSRF tokens in endpoint request handler in com.vaadin:flow-server versions 3.0.0 through 5.0.3 (Vaadin 15.0.0 through 18.0.6), and com.vaadin:fusion-endpoint version 6.0.0 (Vaadin 19.0.0) allows attacker to guess a security token for Fusion endpoints via timing attack. CVE ID : CVE-2021-31406	https://github.com/vaadin/flow/pull/10157 , https://vaadin.com/security/cve-2021-31406	A-VAA-FLOW-040521/387						
vaadin											
Observable Discrepancy	23-04-2021	1.9	Non-constant-time comparison of CSRF tokens in UIDL request handler in com.vaadin:flow-server versions 1.0.0 through 1.0.13 (Vaadin 10.0.0 through 10.0.16), 1.1.0 prior to 2.0.0 (Vaadin 11 prior to 14), 2.0.0 through 2.4.6 (Vaadin 14.0.0 through 14.4.6), 3.0.0 prior to 5.0.0 (Vaadin 15 prior to 18), and 5.0.0 through 5.0.2 (Vaadin 18.0.0 through 18.0.5) allows attacker to guess a security token via timing attack. CVE ID : CVE-2021-31404	https://vaadin.com/security/cve-2021-31404 , https://github.com/vaadin/flow/pull/9875	A-VAA-VAAD-040521/388						
Observable Discrepancy	23-04-2021	1.9	Non-constant-time comparison of CSRF tokens in endpoint request handler in com.vaadin:flow-server	https://github.com/vaadin/flow/pull/10157 ,	A-VAA-VAAD-040521/389						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions 3.0.0 through 5.0.3 (Vaadin 15.0.0 through 18.0.6), and com.vaadin:fusion-endpoint version 6.0.0 (Vaadin 19.0.0) allows attacker to guess a security token for Fusion endpoints via timing attack. CVE ID : CVE-2021-31406	https://vaadin.com/security/cve-2021-31406	
Observable Discrepancy	23-04-2021	1.9	Non-constant-time comparison of CSRF tokens in UIDL request handler in com.vaadin:vaadin-server versions 7.0.0 through 7.7.23 (Vaadin 7.0.0 through 7.7.23), and 8.0.0 through 8.12.2 (Vaadin 8.0.0 through 8.12.2) allows attacker to guess a security token via timing attack CVE ID : CVE-2021-31403	https://vaadin.com/security/cve-2021-31403 , https://github.com/vaadin/framework/pull/12188 , https://github.com/vaadin/framework/pull/12190	A-VAA-VAAD-040521/390
vmware					
nsx-t_data_center					
Improper Privilege Management	19-04-2021	4.6	VMware NSX-T contains a privilege escalation vulnerability due to an issue with RBAC (Role based access control) role assignment. Successful exploitation of this issue may allow attackers with local guest user account to assign privileges higher than their own permission level. CVE ID : CVE-2021-21981	https://www.vmware.com/security/advisories/VMSA-2021-0006.html	A-VMW-NSX--040521/391
webmin					
webmin					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Cross-Site Request Forgery (CSRF)	25-04-2021	6.8	Webmin 1.973 is affected by Cross Site Request Forgery (CSRF) to achieve Remote Command Execution (RCE) through Webmin's running process feature. CVE ID : CVE-2021-31760	N/A	A-WEB-WEBM-040521/392					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-04-2021	6.8	Webmin 1.973 is affected by reflected Cross Site Scripting (XSS) to achieve Remote Command Execution through Webmin's running process feature. CVE ID : CVE-2021-31761	N/A	A-WEB-WEBM-040521/393					
Cross-Site Request Forgery (CSRF)	25-04-2021	6.8	Webmin 1.973 is affected by Cross Site Request Forgery (CSRF) to create a privileged user through Webmin's add users feature, and then get a reverse shell through Webmin's running process feature. CVE ID : CVE-2021-31762	N/A	A-WEB-WEBM-040521/394					
wireshark										
wireshark										
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-04-2021	5	Excessive memory consumption in MS-WSP dissector in Wireshark 3.4.0 to 3.4.4 and 3.2.0 to 3.2.12 allows denial of service via packet injection or crafted capture file CVE ID : CVE-2021-22207	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22207.json , https://www.wireshark.org/security/wnpa-sec-2021-04.html	A-WIR-WIRE-040521/395					
wowza										
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
streaming_engine					
Incorrect Permission Assignment for Critical Resource	23-04-2021	3.6	Wowza Streaming Engine through 4.8.5 (in a default installation) has incorrect file permissions of configuration files in the conf/ directory. A regular local user is able to read and write to all the configuration files, e.g., modify the application server configuration. CVE ID : CVE-2021-31540	https://www.wowza.com/products/streaming-engine	A-WOW-STRE-040521/396
Cleartext Storage of Sensitive Information	23-04-2021	2.1	Wowza Streaming Engine through 4.8.5 (in a default installation) has cleartext passwords stored in the conf/admin.password file. A regular local user is able to read usernames and passwords. CVE ID : CVE-2021-31539	https://www.wowza.com/products/streaming-engine	A-WOW-STRE-040521/397
wrongthink_project					
wrongthink					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2021	4.3	Wrongthink is an encrypted peer-to-peer chat program. A user could check their fingerprint into the service and enter a script to run arbitrary JavaScript on the site. No workarounds exist, but a patch exists in version 2.4.1. CVE ID : CVE-2021-29467	https://github.com/birb-digital/wrongthink/security/advisories/GHSA-529v-f2gf-62w9	A-WRO-WRON-040521/398
xmbforum2					
xmb					
Improper Neutralization of Input During Web	19-04-2021	4.3	XMB is vulnerable to cross-site scripting (XSS) due to inadequate filtering of BBCode input. This bug	https://www.xmbforum2.com/ , https://docs	A-XMB-XMB-040521/399

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
Page Generation ('Cross-site Scripting')			affects all versions of XMB. All XMB installations must be updated to versions 1.9.12.03 or 1.9.11.16. CVE ID : CVE-2021-29399	.xmbforum2.com/index.php?title=Security_Issue_History, https://forums.xmbforum2.com/viewthread.php?tid=777105							
xmlhttprequest-ssl_project											
xmlhttprequest-ssl											
Improper Certificate Validation	23-04-2021	5.8	The xmlhttprequest-ssl package before 1.6.1 for Node.js disables SSL certificate validation by default, because rejectUnauthorized (when the property exists but is undefined) is considered to be false within the https.request function of Node.js. In other words, no certificate is ever rejected. CVE ID : CVE-2021-31597	https://github.com/mjw-wit/node-XMLHttpRequest/commit/bf53329b61ca6afc5d28f6b8d2dc2e3ca740a9b2	A-XML-XMLH-040521/400						
xscreensaver_project											
xscreensaver											
Improper Privilege Management	21-04-2021	7.2	The Debian xscreensaver 5.42+dfsg1-1 package for XScreenSaver has cap_net_raw enabled for the /usr/libexec/xscreensaver/sonar file, which allows local users to gain privileges because this is arguably incompatible with the design of the Mesa 3D Graphics library dependency. CVE ID : CVE-2021-31523	https://www.openwall.com/lists/oss-security/2021/04/17/1, http://www.openwall.com/lists/oss-security/2021/04/21/3	A-XSC-XSCR-040521/401						
xwiki											
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
xwiki										
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-04-2021	4.3	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. It is possible to persistently inject scripts in XWiki versions prior to 12.6.3 and 12.8. Unregistered users can fill simple text fields. Registered users can fill in their personal information and (if they have edit rights) fill the values of static lists using App Within Minutes. There is no easy workaround except upgrading XWiki. The vulnerability has been patched on XWiki 12.8 and 12.6.3. CVE ID : CVE-2021-29459	https://github.com/xwiki/xwiki-platform/security/advisories/GHSA-5c66-v29h-xjh8	A-XWI-XWIK-040521/402					
zohocorp										
manageengine_opmanager										
Deserialization of Untrusted Data	22-04-2021	7.5	Zoho ManageEngine OpManager before 12.5.329 allows unauthenticated Remote Code Execution due to a general bypass in the deserialization class. CVE ID : CVE-2021-3287	https://www.manageengine.com/network-monitoring/help/read-me-complete.html#125329	A-ZOH-MANA-040521/403					
Hardware										
adtran										
netvanta_7060										
Improper Neutralization of Input During Web Page	20-04-2021	3.5	** UNSUPPORTED WHEN ASSIGNED ** The AdTran Personal Phone Manager software is vulnerable to an authenticated stored cross-	http://adtran.com	H-ADT-NETV-040521/404					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
Generation ('Cross-site Scripting')			site scripting (XSS) issues. These issues impact at minimum versions 10.8.1 and below but potentially impact later versions as well since they have not previously been disclosed. Only version 10.8.1 was able to be confirmed during primary research. NOTE: The affected appliances NetVanta 7060 and NetVanta 7100 are considered End of Life and as such this issue will not be patched. CVE ID : CVE-2021-25679								
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-04-2021	4.3	** UNSUPPORTED WHEN ASSIGNED ** The AdTran Personal Phone Manager software is vulnerable to multiple reflected cross-site scripting (XSS) issues. These issues impact at minimum versions 10.8.1 and below but potentially impact later versions as well since they have not previously been disclosed. Only version 10.8.1 was able to be confirmed during primary research. NOTE: The affected appliances NetVanta 7060 and NetVanta 7100 are considered End of Life and as such this issue will not be patched. CVE ID : CVE-2021-25680	http://adtran.com	H-ADT-NETV-040521/405						
N/A	20-04-2021	5	** UNSUPPORTED WHEN ASSIGNED ** AdTran Personal Phone Manager 10.8.1 software is	http://adtran.com	H-ADT-NETV-040521/406						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerable to an issue that allows for exfiltration of data over DNS. This could allow for exposed AdTran Personal Phone Manager web servers to be used as DNS redirectors to tunnel arbitrary data over DNS. NOTE: The affected appliances NetVanta 7060 and NetVanta 7100 are considered End of Life and as such this issue will not be patched. CVE ID : CVE-2021-25681		
netvanta_7100					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-04-2021	3.5	** UNSUPPORTED WHEN ASSIGNED ** The AdTran Personal Phone Manager software is vulnerable to an authenticated stored cross-site scripting (XSS) issues. These issues impact at minimum versions 10.8.1 and below but potentially impact later versions as well since they have not previously been disclosed. Only version 10.8.1 was able to be confirmed during primary research. NOTE: The affected appliances NetVanta 7060 and NetVanta 7100 are considered End of Life and as such this issue will not be patched. CVE ID : CVE-2021-25679	http://adtran.com	H-ADT-NETV-040521/407
Improper Neutralization of Input During Web	20-04-2021	4.3	** UNSUPPORTED WHEN ASSIGNED ** The AdTran Personal Phone Manager software is vulnerable to	http://adtran.com	H-ADT-NETV-040521/408

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Page Generation ('Cross-site Scripting')			multiple reflected cross-site scripting (XSS) issues. These issues impact at minimum versions 10.8.1 and below but potentially impact later versions as well since they have not previously been disclosed. Only version 10.8.1 was able to be confirmed during primary research. NOTE: The affected appliances NetVanta 7060 and NetVanta 7100 are considered End of Life and as such this issue will not be patched. CVE ID : CVE-2021-25680							
N/A	20-04-2021	5	** UNSUPPORTED WHEN ASSIGNED ** AdTran Personal Phone Manager 10.8.1 software is vulnerable to an issue that allows for exfiltration of data over DNS. This could allow for exposed AdTran Personal Phone Manager web servers to be used as DNS redirectors to tunnel arbitrary data over DNS. NOTE: The affected appliances NetVanta 7060 and NetVanta 7100 are considered End of Life and as such this issue will not be patched. CVE ID : CVE-2021-25681	http://adtran.com	H-ADT-NETV-040521/409					
aterm										
wg2600hs										
Improper Neutralization of Input	26-04-2021	4.3	Cross-site scripting vulnerability in Aterm WG2600HS firmware	N/A	H-ATE-WG26-040521/410					
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
During Web Page Generation ('Cross-site Scripting')			Ver1.5.1 and earlier allows remote attackers to inject an arbitrary script via unspecified vectors. CVE ID : CVE-2021-20710		
fibaro					
home_center_2					
Incorrect Authorization	19-04-2021	7.8	In Fibaro Home Center 2 and Lite devices with firmware version 4.600 and older an internal management service is accessible on port 8000 and some API endpoints could be accessed without authentication to trigger a shutdown, a reboot or a reboot into recovery mode. CVE ID : CVE-2021-20990	https://www.iot-inspector.com/blog/advisory-fibaro-home-center/	H-FIB-HOME-040521/411
Cleartext Transmission of Sensitive Information	19-04-2021	5	In Fibaro Home Center 2 and Lite devices in all versions provide a web based management interface over unencrypted HTTP protocol. Communication between the user and the device can be eavesdropped to hijack sessions, tokens and passwords. CVE ID : CVE-2021-20992	https://www.iot-inspector.com/blog/advisory-fibaro-home-center/	H-FIB-HOME-040521/412
Missing Authorization	19-04-2021	4.3	Fibaro Home Center 2 and Lite devices with firmware version 4.600 and older initiate SSH connections to the Fibaro cloud to provide remote access and remote support capabilities. This connection can be intercepted using DNS spoofing attack and a device	https://www.iot-inspector.com/blog/advisory-fibaro-home-center/	H-FIB-HOME-040521/413

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			initiated remote port-forward channel can be used to connect to the web management interface. Knowledge of authorization credentials to the management interface is required to perform any further actions. CVE ID : CVE-2021-20989		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-04-2021	9	In Fibaro Home Center 2 and Lite devices with firmware version 4.540 and older an authenticated user can run commands as root user using a command injection vulnerability. CVE ID : CVE-2021-20991	https://www.iot-inspector.com/blog/advisory-fibaro-home-center/	H-FIB-HOME-040521/414
home_center_lite					
Incorrect Authorization	19-04-2021	7.8	In Fibaro Home Center 2 and Lite devices with firmware version 4.600 and older an internal management service is accessible on port 8000 and some API endpoints could be accessed without authentication to trigger a shutdown, a reboot or a reboot into recovery mode. CVE ID : CVE-2021-20990	https://www.iot-inspector.com/blog/advisory-fibaro-home-center/	H-FIB-HOME-040521/415
Cleartext Transmission of Sensitive Information	19-04-2021	5	In Fibaro Home Center 2 and Lite devices in all versions provide a web based management interface over unencrypted HTTP protocol. Communication between the user and the device can be eavesdropped to hijack sessions, tokens and	https://www.iot-inspector.com/blog/advisory-fibaro-home-center/	H-FIB-HOME-040521/416

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			passwords. CVE ID : CVE-2021-20992							
Missing Authorization	19-04-2021	4.3	Fibaro Home Center 2 and Lite devices with firmware version 4.600 and older initiate SSH connections to the Fibaro cloud to provide remote access and remote support capabilities. This connection can be intercepted using DNS spoofing attack and a device initiated remote port-forward channel can be used to connect to the web management interface. Knowledge of authorization credentials to the management interface is required to perform any further actions. CVE ID : CVE-2021-20989	https://www.iot-inspector.com/blog/advisory-fibaro-home-center/	H-FIB-HOME-040521/417					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-04-2021	9	In Fibaro Home Center 2 and Lite devices with firmware version 4.540 and older an authenticated user can run commands as root user using a command injection vulnerability. CVE ID : CVE-2021-20991	https://www.iot-inspector.com/blog/advisory-fibaro-home-center/	H-FIB-HOME-040521/418					
jtekt										
2port-efr_thu-6404										
Improper Resource Shutdown or Release	19-04-2021	5	If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All	N/A	H-JTE-2POR-040521/419					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters.</p> <p>CVE ID : CVE-2021-27458</p>		
fl\\et-t-v2h_thu-6289					
Improper Resource Shutdown or Release	19-04-2021	5	<p>If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions,</p>	N/A	H-JTE-FL\\-040521/420

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters. CVE ID : CVE-2021-27458		
pc10b_tcc-1021					
Improper Resource Shutdown or Release	19-04-2021	5	If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E	N/A	H-JTE-PC10-040521/421

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU- 6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU- 6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC- PC3J/PC2J Series: FL/ET-T- V2H THU-6289: All versions, 2PORT-EFR THU- 6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters.</p> <p>CVE ID : CVE-2021-27458</p>		
pc10b-e\\c_tcu-6521					
Improper Resource Shutdown or Release	19-04-2021	5	<p>If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC- 6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC- 6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU- 6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions,</p>	N/A	H-JTE-PC10- 040521/422

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters.</p> <p>CVE ID : CVE-2021-27458</p>		

pc10b-p_tcc-6373

Improper Resource Shutdown or Release	19-04-2021	5	<p>If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR</p>	N/A	H-JTE-PC10-040521/423
---------------------------------------	------------	---	---	-----	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters. CVE ID : CVE-2021-27458		

pc10e_tcc-4737

Improper Resource Shutdown or Release	19-04-2021	5	If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-	N/A	H-JTE-PC10-040521/424
---------------------------------------	------------	---	---	-----	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters. CVE ID : CVE-2021-27458		
pc10g-cpu_tcc-6353					
Improper Resource Shutdown or Release	19-04-2021	5	If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-	N/A	H-JTE-PC10-040521/425

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters. CVE ID : CVE-2021-27458		
pc10ge_tcc-6464					
Improper Resource Shutdown or Release	19-04-2021	5	If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-	N/A	H-JTE-PC10-040521/426

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters. CVE ID : CVE-2021-27458		
pc10p_tcc-6372					
Improper Resource Shutdown or Release	19-04-2021	5	If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-6404: All versions) are left in an open state by an attacker, Ethernet	N/A	H-JTE-PC10-040521/427

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
			communications cannot be established with other devices, depending on the settings of the link parameters. CVE ID : CVE-2021-27458		
pc10p-dp_tcc-6726					
Improper Resource Shutdown or Release	19-04-2021	5	If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the	N/A	H-JTE-PC10-040521/428

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			settings of the link parameters. CVE ID : CVE-2021-27458		
pc10p-dp-io_tcc-6752					
Improper Resource Shutdown or Release	19-04-2021	5	If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters.	N/A	H-JTE-PC10-040521/429

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-27458		
plus_2p-efr_tcu-6929					
Improper Resource Shutdown or Release	19-04-2021	5	<p>If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters.</p> <p>CVE ID : CVE-2021-27458</p>	N/A	H-JTE-PLUS-040521/430
plus_bus-ex_tcu-6900					

CVSS Scoring Scale	0-1	1-2	2-3	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 Resource Shutdown or Release	19-04-2021	5	<p>If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters.</p> <p>CVE ID : CVE-2021-27458</p>	N/A	H-JTE-PLUS-040521/431
plus_cpu_tcc-6740					
Improper Resource Shutdown or	19-04-2021	5	If Ethernet communication of the JTEKT Corporation TOYOPUC product series'	N/A	H-JTE-PLUS-040521/432

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Release			<p>(TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters.</p> <p>CVE ID : CVE-2021-27458</p>		
plus_efr_tcu-6743					
Improper Resource Shutdown or Release	19-04-2021	5	<p>If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-</p>	N/A	H-JTE-PLUS-040521/433

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters.</p> <p>CVE ID : CVE-2021-27458</p>		
plus_efr2_tcu-6859					
Improper Resource Shutdown or Release	19-04-2021	5	<p>If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All</p>	N/A	H-JTE-PLUS-040521/434

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters.</p> <p>CVE ID : CVE-2021-27458</p>		
plus_ex_tcu-6741					
Improper Resource Shutdown or Release	19-04-2021	5	<p>If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions,</p>	N/A	H-JTE-PLUS-040521/435

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters. CVE ID : CVE-2021-27458		
plus_ex2_tcu-6858					
Improper Resource Shutdown or Release	19-04-2021	5	If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E	N/A	H-JTE-PLUS-040521/436

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU- 6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU- 6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC- PC3J/PC2J Series: FL/ET-T- V2H THU-6289: All versions, 2PORT-EFR THU- 6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters.</p> <p>CVE ID : CVE-2021-27458</p>		
juniper					
acx4000					
Uncontrolled Resource Consumption	22-04-2021	5	<p>A vulnerability in Juniper Networks Junos OS ACX500 Series, ACX4000 Series, may allow an attacker to cause a Denial of Service (DoS) by sending a high rate of specific packets to the device, resulting in a Forwarding Engine Board (FFEB) crash. Continued receipt of these packets will sustain the Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS on ACX500 Series, ACX4000 Series: 17.4</p>	https://kb.juniper.net/JS_A11128	H-JUN-ACX4-040521/437

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 17.4R3-S2. CVE ID : CVE-2021-0233		
acx500					
Uncontrolled Resource Consumption	22-04-2021	5	A vulnerability in Juniper Networks Junos OS ACX500 Series, ACX4000 Series, may allow an attacker to cause a Denial of Service (DoS) by sending a high rate of specific packets to the device, resulting in a Forwarding Engine Board (FFEB) crash. Continued receipt of these packets will sustain the Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS on ACX500 Series, ACX4000 Series: 17.4 versions prior to 17.4R3-S2. CVE ID : CVE-2021-0233	https://kb.juniper.net/JS_A11128	H-JUN-ACX5-040521/438
acx5448					
Uncontrolled Resource Consumption	22-04-2021	5	A vulnerability in Juniper Networks Junos OS running on the ACX5448 and ACX710 platforms may cause BFD sessions to flap when a high rate of transit ARP packets are received. This, in turn, may impact routing protocols and network stability, leading to a Denial of Service (DoS) condition. When a high rate of transit ARP packets are exceptioned to the CPU and BFD flaps, the following log messages may be seen: bfdd[15864]: BFDD_STATE_UP_TO_DOW N: BFD Session 192.168.14.3 (IFL 232)	https://kb.juniper.net/JS_A11118	H-JUN-ACX5-040521/439

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>state Up -> Down LD/RD(17/19) Up time:11:38:17 Local diag: CtlExpire Remote diag: None Reason: Detect Timer Expiry. bfdd[15864]: BFDD_TRAP_SHOP_STATE_ DOWN: local discriminator: 17, new state: down, interface: irb.998, peer addr: 192.168.14.3 rpd[15839]: RPD_ISIS_ADJDOWN: IS-IS lost L2 adjacency to peer on irb.998, reason: BFD Session Down bfdd[15864]: BFDD_TRAP_SHOP_STATE_ UP: local discriminator: 17, new state: up, interface: irb.998, peer addr: 192.168.14.3 This issue only affects the ACX5448 Series and ACX710 Series routers. No other products or platforms are affected by this vulnerability. This issue affects Juniper Networks Junos OS: 18.2 versions prior to 18.2R3-S8 on ACX5448; 18.3 versions prior to 18.3R3-S5 on ACX5448; 18.4 versions prior to 18.4R1-S6, 18.4R3- S7 on ACX5448; 19.1 versions prior to 19.1R3-S5 on ACX5448; 19.2 versions prior to 19.2R2, 19.2R3 on ACX5448; 19.3 versions prior to 19.3R3 on ACX5448; 19.4 versions prior to 19.4R3 on ACX5448; 20.1 versions prior to 20.1R2 on ACX5448; 20.2 versions</p>		

CVSS Scoring Scale	0-1	1-2	2-3	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 20.2R2 on ACX5448 and ACX710. CVE ID : CVE-2021-0216		
acx6360					
Uncontrolled Resource Consumption	22-04-2021	5	On Juniper Networks Junos OS platforms with link aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel: rt_pfe_veto: Memory over consumed. Op 1 err 12, rtsm_id 0:-1, msg type 72 /kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<< user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests	https://kb.juniper.net/JS_A11125	H-JUN-ACX6-040521/440

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<< This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000- 72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3.</p> <p>CVE ID : CVE-2021-0230</p>		

acx710

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	22-04-2021	5	<p>A vulnerability in Juniper Networks Junos OS running on the ACX5448 and ACX710 platforms may cause BFD sessions to flap when a high rate of transit ARP packets are received. This, in turn, may impact routing protocols and network stability, leading to a Denial of Service (DoS) condition. When a high rate of transit ARP packets are exceptioned to the CPU and BFD flaps, the following log messages may be seen:</p> <pre> bfdd[15864]: BFDD_STATE_UP_TO_DOWN: BFD Session 192.168.14.3 (IFL 232) state Up -> Down LD/RD(17/19) Up time:11:38:17 Local diag: CtlExpire Remote diag: None Reason: Detect Timer Expiry. bfdd[15864]: BFDD_TRAP_SHOP_STATE_DOWN: local discriminator: 17, new state: down, interface: irb.998, peer addr: 192.168.14.3 rpd[15839]: RPD_ISIS_ADJDOWN: IS-IS lost L2 adjacency to peer on irb.998, reason: BFD Session Down bfdd[15864]: BFDD_TRAP_SHOP_STATE_UP: local discriminator: 17, new state: up, interface: irb.998, peer addr: 192.168.14.3 This issue only affects the ACX5448 Series and ACX710 Series routers. No other products </pre>	https://kb.juniper.net/JS_A11118	H-JUN-ACX7-040521/441

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>or platforms are affected by this vulnerability. This issue affects Juniper Networks Junos OS: 18.2 versions prior to 18.2R3-S8 on ACX5448; 18.3 versions prior to 18.3R3-S5 on ACX5448; 18.4 versions prior to 18.4R1-S6, 18.4R3-S7 on ACX5448; 19.1 versions prior to 19.1R3-S5 on ACX5448; 19.2 versions prior to 19.2R2, 19.2R3 on ACX5448; 19.3 versions prior to 19.3R3 on ACX5448; 19.4 versions prior to 19.4R3 on ACX5448; 20.1 versions prior to 20.1R2 on ACX5448; 20.2 versions prior to 20.2R2 on ACX5448 and ACX710.</p> <p>CVE ID : CVE-2021-0216</p>		
Uncontrolled Resource Consumption	22-04-2021	5	<p>On Juniper Networks Junos OS platforms with link aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel: rt_pfe_veto: Memory over consumed. Op 1 err 12, rtsm_id 0:-1, msg type 72 /kernel: rt_pfe_veto: free</p>	https://kb.juniper.net/JS_A11125	H-JUN-ACX7-040521/442

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>kmem_map memory = (20770816) curproc = kmd An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<< user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<< This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000-72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3</p>		

CVSS Scoring Scale	0-1	1-2	2-3	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 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3. CVE ID : CVE-2021-0230		
csrx					
Use of Hard-coded Credentials	22-04-2021	7.5	The use of multiple hard-coded cryptographic keys in cSRX Series software in Juniper Networks Junos OS allows an attacker to take control of any instance of a cSRX deployment through device management services. This issue affects: Juniper Networks Junos OS on cSRX Series: All versions prior to 20.2R3; 20.3 versions prior to 20.3R2; 20.4 versions prior to 20.4R2. CVE ID : CVE-2021-0266	https://kb.juniper.net/JS_A11157	H-JUN-CSRX-040521/443
ex2200-c					
Double Free	22-04-2021	5	A Double Free vulnerability in the software forwarding interface daemon (sfid) process of Juniper Networks Junos OS allows an adjacently-connected attacker to cause a Denial of	https://kb.juniper.net/JS_A11162	H-JUN-EX22-040521/444

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Service (DoS) by sending a crafted ARP packet to the device. Continued receipt and processing of the crafted ARP packets will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX2200-C Series, EX3200 Series, EX3300 Series, EX4200 Series, EX4500 Series, EX4550 Series, EX6210 Series, EX8208 Series, EX8216 Series. 12.3 versions prior to 12.3R12-S17; 15.1 versions prior to 15.1R7-S8. This issue only affects the listed Marvell-chipset based EX Series devices. No other products or platforms are affected.</p> <p>CVE ID : CVE-2021-0271</p>		
ex2300					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	4.3	<p>A signal handler race condition exists in the Layer 2 Address Learning Daemon (L2ALD) of Juniper Networks Junos OS due to the absence of a specific protection mechanism to avoid a race condition which may allow an attacker to bypass the storm-control feature on devices. This issue is a corner case and only occurs during specific actions taken by an administrator of a device under certain specific actions which triggers the event. The event occurs less frequently</p>	https://kb.juniper.net/JS_A11137	H-JUN-EX23-040521/445

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>on devices which are not configured with Virtual Chassis configurations, and more frequently on devices configured in Virtual Chassis configurations. This issue is not specific to any particular Junos OS platform. An Indicator of Compromise (IoC) may be seen by reviewing log files for the following error message seen by executing the following show statement: show log messages grep storm</p> <p>Result to look for: /kernel: GENCFG: op 58 (Storm Control Blob) failed; err 1 (Unknown) This issue affects: Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D49 on EX Series; 15.1 versions prior to 15.1R7-S6; 15.1X49 versions prior to 15.1X49-D191, 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3; 17.2 versions prior to 17.2R2-S8, 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S5; 18.2 versions prior to 18.2R2-S6, 18.2R3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R1-S5, 18.4R2; 19.1</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 19.1R1-S4, 19.1R2. CVE ID : CVE-2021-0244		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2021	9.3	A Cross-site Scripting (XSS) vulnerability in J-Web on Juniper Networks Junos OS allows an attacker to target another user's session thereby gaining access to the users session. The other user session must be active for the attack to succeed. Once successful, the attacker has the same privileges as the user. If the user has root privileges, the attacker may be able to gain full control of the device. This issue affects: Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S15 on EX Series; 12.3X48 versions prior to 12.3X48-D95 on SRX Series; 15.1 versions prior to 15.1R7-S6 on EX Series; 15.1X49 versions prior to 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1; 18.4 versions	https://kb.juniper.net/JS_A11166	H-JUN-EX23-040521/446

CVSS Scoring Scale	0-1	1-2	2-3	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 18.4R1-S6, 18.4R2-S4, 18.4R3; 19.1 versions prior to 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S3, 19.2R2; 19.3 versions prior to 19.3R2. CVE ID : CVE-2021-0275		
ex2300-c					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	4.3	A signal handler race condition exists in the Layer 2 Address Learning Daemon (L2ALD) of Juniper Networks Junos OS due to the absence of a specific protection mechanism to avoid a race condition which may allow an attacker to bypass the storm-control feature on devices. This issue is a corner case and only occurs during specific actions taken by an administrator of a device under certain specific actions which triggers the event. The event occurs less frequently on devices which are not configured with Virtual Chassis configurations, and more frequently on devices configured in Virtual Chassis configurations. This issue is not specific to any particular Junos OS platform. An Indicator of Compromise (IoC) may be seen by reviewing log files for the following error message seen by executing the following show statement: show log messages grep storm	https://kb.juniper.net/JS_A11137	H-JUN-EX23-040521/447

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Result to look for: /kernel: GENCFG: op 58 (Storm Control Blob) failed; err 1 (Unknown) This issue affects: Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D49 on EX Series; 15.1 versions prior to 15.1R7-S6; 15.1X49 versions prior to 15.1X49-D191, 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3; 17.2 versions prior to 17.2R2-S8, 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S5; 18.2 versions prior to 18.2R2-S6, 18.2R3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R1-S5, 18.4R2; 19.1 versions prior to 19.1R1-S4, 19.1R2.</p> <p>CVE ID : CVE-2021-0244</p>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2021	9.3	<p>A Cross-site Scripting (XSS) vulnerability in J-Web on Juniper Networks Junos OS allows an attacker to target another user's session thereby gaining access to the users session. The other user session must be active for the attack to succeed. Once successful, the attacker has the same privileges as the user. If the</p>	https://kb.juniper.net/JS_A11166	H-JUN-EX23-040521/448

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>user has root privileges, the attacker may be able to gain full control of the device. This issue affects: Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S15 on EX Series; 12.3X48 versions prior to 12.3X48-D95 on SRX Series; 15.1 versions prior to 15.1R7-S6 on EX Series; 15.1X49 versions prior to 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3; 19.1 versions prior to 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S3, 19.2R2; 19.3 versions prior to 19.3R2.</p> <p>CVE ID : CVE-2021-0275</p>		
ex3200					
Double Free	22-04-2021	5	<p>A Double Free vulnerability in the software forwarding interface daemon (sfid) process of Juniper Networks Junos OS allows an adjacently-connected attacker to cause a Denial of</p>	https://kb.juniper.net/JS_A11162	H-JUN-EX32-040521/449

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Service (DoS) by sending a crafted ARP packet to the device. Continued receipt and processing of the crafted ARP packets will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX2200-C Series, EX3200 Series, EX3300 Series, EX4200 Series, EX4500 Series, EX4550 Series, EX6210 Series, EX8208 Series, EX8216 Series. 12.3 versions prior to 12.3R12-S17; 15.1 versions prior to 15.1R7-S8. This issue only affects the listed Marvell-chipset based EX Series devices. No other products or platforms are affected.</p> <p>CVE ID : CVE-2021-0271</p>		

ex3300

Double Free	22-04-2021	5	<p>A Double Free vulnerability in the software forwarding interface daemon (sfid) process of Juniper Networks Junos OS allows an adjacently-connected attacker to cause a Denial of Service (DoS) by sending a crafted ARP packet to the device. Continued receipt and processing of the crafted ARP packets will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX2200-C Series, EX3200 Series, EX3300 Series, EX4200 Series, EX4500</p>	https://kb.juniper.net/JS_A11162	H-JUN-EX33-040521/450
-------------	------------	---	---	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series, EX4550 Series, EX6210 Series, EX8208 Series, EX8216 Series. 12.3 versions prior to 12.3R12-S17; 15.1 versions prior to 15.1R7-S8. This issue only affects the listed Marvell-chipset based EX Series devices. No other products or platforms are affected. CVE ID : CVE-2021-0271		
ex3400					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	4.3	A signal handler race condition exists in the Layer 2 Address Learning Daemon (L2ALD) of Juniper Networks Junos OS due to the absence of a specific protection mechanism to avoid a race condition which may allow an attacker to bypass the storm-control feature on devices. This issue is a corner case and only occurs during specific actions taken by an administrator of a device under certain specific actions which triggers the event. The event occurs less frequently on devices which are not configured with Virtual Chassis configurations, and more frequently on devices configured in Virtual Chassis configurations. This issue is not specific to any particular Junos OS platform. An Indicator of Compromise (IoC) may be seen by reviewing log files for the following error	https://kb.juniper.net/JS_A11137	H-JUN-EX34-040521/451

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>message seen by executing the following show statement: show log messages grep storm Result to look for: /kernel: GENCFG: op 58 (Storm Control Blob) failed; err 1 (Unknown) This issue affects: Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D49 on EX Series; 15.1 versions prior to 15.1R7-S6; 15.1X49 versions prior to 15.1X49-D191, 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3; 17.2 versions prior to 17.2R2-S8, 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S5; 18.2 versions prior to 18.2R2-S6, 18.2R3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R1-S5, 18.4R2; 19.1 versions prior to 19.1R1-S4, 19.1R2.</p> <p>CVE ID : CVE-2021-0244</p>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2021	9.3	<p>A Cross-site Scripting (XSS) vulnerability in J-Web on Juniper Networks Junos OS allows an attacker to target another user's session thereby gaining access to the users session. The other user session must be active</p>	https://kb.juniper.net/JS_A11166	H-JUN-EX34-040521/452

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			<p>for the attack to succeed. Once successful, the attacker has the same privileges as the user. If the user has root privileges, the attacker may be able to gain full control of the device. This issue affects: Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S15 on EX Series; 12.3X48 versions prior to 12.3X48-D95 on SRX Series; 15.1 versions prior to 15.1R7-S6 on EX Series; 15.1X49 versions prior to 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3; 19.1 versions prior to 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S3, 19.2R2; 19.3 versions prior to 19.3R2.</p> <p>CVE ID : CVE-2021-0275</p>							
ex4200										
Double Free	22-04-2021	5	A Double Free vulnerability in the software forwarding interface daemon (sfid)	https://kb.juniper.net/JS_A11162	H-JUN-EX42-040521/453					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>process of Juniper Networks Junos OS allows an adjacently-connected attacker to cause a Denial of Service (DoS) by sending a crafted ARP packet to the device. Continued receipt and processing of the crafted ARP packets will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX2200-C Series, EX3200 Series, EX3300 Series, EX4200 Series, EX4500 Series, EX4550 Series, EX6210 Series, EX8208 Series, EX8216 Series. 12.3 versions prior to 12.3R12-S17; 15.1 versions prior to 15.1R7-S8. This issue only affects the listed Marvell-chipset based EX Series devices. No other products or platforms are affected.</p> <p>CVE ID : CVE-2021-0271</p>		
ex4300					
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-04-2021	6.1	<p>A vulnerability due to the improper handling of direct memory access (DMA) buffers on EX4300 switches on Juniper Networks Junos OS allows an attacker sending specific unicast frames to trigger a Denial of Service (DoS) condition by exhausting DMA buffers, causing the FPC to crash and the device to restart. The DMA buffer leak is seen when receiving these specific, valid unicast</p>	https://kb.juniper.net/JS_A11135	H-JUN-EX43-040521/454

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>frames on an interface without Layer 2 Protocol Tunneling (L2PT) or dot1x configured. Interfaces with either L2PT or dot1x configured are not vulnerable to this issue. When this issue occurs, DMA buffer usage keeps increasing and the following error log messages may be observed: Apr 14 14:29:34.360 /kernel: pid 64476 (pfex_junos), uid 0: exited on signal 11 (core dumped) Apr 14 14:29:33.790 init: pfe-manager (PID 64476) terminated by signal number 11. Core dumped! The DMA buffers on the FPC can be monitored by the executing vty command 'show heap':</p> <pre>ID Base Total(b) Free(b) Used(b) % Name -- -----</pre> <pre>----- 0 4a46000 268435456 238230496 30204960 11 Kernel 1 18a46000 67108864 17618536 49490328 73 Bcm_sdk 2 23737000 117440512 18414552 99025960 84 DMA buf <<<<< keeps increasing 3 2a737000 16777216 16777216 0 0 DMA desc This issue affects Juniper Networks Junos OS on the EX4300: 17.3 versions prior to 17.3R3- S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to</pre>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S1, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. CVE ID : CVE-2021-0242		
N/A	22-04-2021	3.3	Improper Handling of Unexpected Data in the firewall policer of Juniper Networks Junos OS on EX4300 switches allows matching traffic to exceed set policer limits, possibly leading to a limited Denial of Service (DoS) condition. When the firewall policer discard action fails on a Layer 2 port, it will allow traffic to pass even though it exceeds set policer limits. Traffic will not get discarded, and will be forwarded even though a policer discard action is configured. When the issue occurs, traffic is not discarded as desired, which can be observed by comparing the Input bytes with the Output bytes using the following command:	https://kb.juniper.net/JS_A11136	H-JUN-EX43-040521/455

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>user@junos> monitor interface traffic Interface Link Input bytes (bps) Output bytes (bps) ge-0/0/0 Up 37425422 (82616) 37425354 (82616) <<<< egress ge-0/0/1 Up 37425898 (82616) 37425354 (82616) <<<< ingress The expected output, with input and output counters differing, is shown below: Interface Link Input bytes (bps) Output bytes (bps) ge-0/0/0 Up 342420570 (54600) 342422760 (54600) <<<< egress ge-0/0/1 Up 517672120 (84000) 342420570 (54600) <<<< ingress This issue only affects IPv4 policing. IPv6 traffic and firewall policing actions are not affected by this issue. This issue affects Juniper Networks Junos OS on the EX4300: All versions prior to 17.3R3-S10; 17.4 versions prior to 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S6; 19.1 versions prior to 19.1R3-S3; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2.</p>		

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-0243							
Concurrent Execution using Shared Resource with Improper Synchronizati on ('Race Condition')	22-04-2021	4.3	A signal handler race condition exists in the Layer 2 Address Learning Daemon (L2ALD) of Juniper Networks Junos OS due to the absence of a specific protection mechanism to avoid a race condition which may allow an attacker to bypass the storm-control feature on devices. This issue is a corner case and only occurs during specific actions taken by an administrator of a device under certain specifics actions which triggers the event. The event occurs less frequently on devices which are not configured with Virtual Chassis configurations, and more frequently on devices configured in Virtual Chassis configurations. This issue is not specific to any particular Junos OS platform. An Indicator of Compromise (IoC) may be seen by reviewing log files for the following error message seen by executing the following show statement: show log messages grep storm Result to look for: /kernel: GENCFG: op 58 (Storm Control Blob) failed; err 1 (Unknown) This issue affects: Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D49 on EX Series; 15.1 versions prior	https://kb.juniper.net/JS_A11137	H-JUN-EX43-040521/456					
CVSS Scoring Scale										
	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

0-1

1-2

2-3

3-4

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to 15.1R7-S6; 15.1X49 versions prior to 15.1X49-D191, 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3; 17.2 versions prior to 17.2R2-S8, 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S5; 18.2 versions prior to 18.2R2-S6, 18.2R3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R1-S5, 18.4R2; 19.1 versions prior to 19.1R1-S4, 19.1R2. CVE ID : CVE-2021-0244		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2021	9.3	A Cross-site Scripting (XSS) vulnerability in J-Web on Juniper Networks Junos OS allows an attacker to target another user's session thereby gaining access to the users session. The other user session must be active for the attack to succeed. Once successful, the attacker has the same privileges as the user. If the user has root privileges, the attacker may be able to gain full control of the device. This issue affects: Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S15 on EX Series; 12.3X48 versions prior to 12.3X48-	https://kb.juniper.net/JS_A11166	H-JUN-EX43-040521/457

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			D95 on SRX Series; 15.1 versions prior to 15.1R7-S6 on EX Series; 15.1X49 versions prior to 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3; 19.1 versions prior to 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S3, 19.2R2; 19.3 versions prior to 19.3R2. CVE ID : CVE-2021-0275		
ex4300-mp					
N/A	22-04-2021	5	On Juniper Networks EX4300-MP Series, EX4600 Series, EX4650 Series, QFX5K Series deployed as a Virtual Chassis with a specific Layer 2 circuit configuration, Packet Forwarding Engine manager (FXPC) process may crash and restart upon receipt of specific layer 2 frames. Continued receipt and processing of this packet will create a sustained Denial of Service	https://kb.juniper.net/JS_A11132	H-JUN-EX43-040521/458

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP Series, EX4600 Series, EX4650 Series, QFX5K Series 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4, 17.4R3-S5; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2; CVE ID : CVE-2021-0237		
ex4400					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	4.3	A signal handler race condition exists in the Layer 2 Address Learning Daemon (L2ALD) of Juniper Networks Junos OS due to the absence of a specific protection mechanism to avoid a race condition which may allow an attacker to bypass the storm-control feature on devices. This issue is a corner case and only occurs during specific actions taken by an administrator of a device under certain	https://kb.juniper.net/JS_A11137	H-JUN-EX44-040521/459

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>specifics actions which triggers the event. The event occurs less frequently on devices which are not configured with Virtual Chassis configurations, and more frequently on devices configured in Virtual Chassis configurations. This issue is not specific to any particular Junos OS platform. An Indicator of Compromise (IoC) may be seen by reviewing log files for the following error message seen by executing the following show statement: show log messages grep storm</p> <p>Result to look for: /kernel: GENCFG: op 58 (Storm Control Blob) failed; err 1 (Unknown) This issue affects: Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D49 on EX Series; 15.1 versions prior to 15.1R7-S6; 15.1X49 versions prior to 15.1X49-D191, 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3; 17.2 versions prior to 17.2R2-S8, 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S5; 18.2 versions prior to 18.2R2-S6, 18.2R3; 18.3 versions prior to</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.3R1-S7, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R1-S5, 18.4R2; 19.1 versions prior to 19.1R1-S4, 19.1R2. CVE ID : CVE-2021-0244		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2021	9.3	A Cross-site Scripting (XSS) vulnerability in J-Web on Juniper Networks Junos OS allows an attacker to target another user's session thereby gaining access to the users session. The other user session must be active for the attack to succeed. Once successful, the attacker has the same privileges as the user. If the user has root privileges, the attacker may be able to gain full control of the device. This issue affects: Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S15 on EX Series; 12.3X48 versions prior to 12.3X48-D95 on SRX Series; 15.1 versions prior to 15.1R7-S6 on EX Series; 15.1X49 versions prior to 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R2-S7, 18.2R3-	https://kb.juniper.net/JS_A11166	H-JUN-EX44-040521/460

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3; 19.1 versions prior to 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S3, 19.2R2; 19.3 versions prior to 19.3R2. CVE ID : CVE-2021-0275		

ex4500

Double Free	22-04-2021	5	A Double Free vulnerability in the software forwarding interface daemon (sfid) process of Juniper Networks Junos OS allows an adjacently-connected attacker to cause a Denial of Service (DoS) by sending a crafted ARP packet to the device. Continued receipt and processing of the crafted ARP packets will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX2200-C Series, EX3200 Series, EX3300 Series, EX4200 Series, EX4500 Series, EX4550 Series, EX6210 Series, EX8208 Series, EX8216 Series. 12.3 versions prior to 12.3R12-S17; 15.1 versions prior to 15.1R7-S8. This issue only affects the listed Marvell-chipset based EX Series devices. No other products or platforms are affected. CVE ID : CVE-2021-0271	https://kb.juniper.net/JS_A11162	H-JUN-EX45-040521/461
-------------	------------	---	--	---	-----------------------

ex4550

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	22-04-2021	5	<p>A Double Free vulnerability in the software forwarding interface daemon (sfid) process of Juniper Networks Junos OS allows an adjacently-connected attacker to cause a Denial of Service (DoS) by sending a crafted ARP packet to the device. Continued receipt and processing of the crafted ARP packets will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX2200-C Series, EX3200 Series, EX3300 Series, EX4200 Series, EX4500 Series, EX4550 Series, EX6210 Series, EX8208 Series, EX8216 Series. 12.3 versions prior to 12.3R12-S17; 15.1 versions prior to 15.1R7-S8. This issue only affects the listed Marvell-chipset based EX Series devices. No other products or platforms are affected.</p> <p>CVE ID : CVE-2021-0271</p>	https://kb.juniper.net/JS_A11162	H-JUN-EX45-040521/462
ex4600					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	4.3	<p>A signal handler race condition exists in the Layer 2 Address Learning Daemon (L2ALD) of Juniper Networks Junos OS due to the absence of a specific protection mechanism to avoid a race condition which may allow an attacker to bypass the storm-control feature on devices. This issue is a</p>	https://kb.juniper.net/JS_A11137	H-JUN-EX46-040521/463

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>corner case and only occurs during specific actions taken by an administrator of a device under certain specifics actions which triggers the event. The event occurs less frequently on devices which are not configured with Virtual Chassis configurations, and more frequently on devices configured in Virtual Chassis configurations. This issue is not specific to any particular Junos OS platform. An Indicator of Compromise (IoC) may be seen by reviewing log files for the following error message seen by executing the following show statement: show log messages grep storm</p> <p>Result to look for: /kernel: GENCFG: op 58 (Storm Control Blob) failed; err 1 (Unknown) This issue affects: Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D49 on EX Series; 15.1 versions prior to 15.1R7-S6; 15.1X49 versions prior to 15.1X49-D191, 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3; 17.2 versions prior to 17.2R2-S8, 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9,</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			17.4R3; 18.1 versions prior to 18.1R3-S5; 18.2 versions prior to 18.2R2-S6, 18.2R3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R1-S5, 18.4R2; 19.1 versions prior to 19.1R1-S4, 19.1R2. CVE ID : CVE-2021-0244		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2021	9.3	A Cross-site Scripting (XSS) vulnerability in J-Web on Juniper Networks Junos OS allows an attacker to target another user's session thereby gaining access to the users session. The other user session must be active for the attack to succeed. Once successful, the attacker has the same privileges as the user. If the user has root privileges, the attacker may be able to gain full control of the device. This issue affects: Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S15 on EX Series; 12.3X48 versions prior to 12.3X48-D95 on SRX Series; 15.1 versions prior to 15.1R7-S6 on EX Series; 15.1X49 versions prior to 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4	https://kb.juniper.net/JS_A11166	H-JUN-EX46-040521/464

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3; 19.1 versions prior to 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S3, 19.2R2; 19.3 versions prior to 19.3R2. CVE ID : CVE-2021-0275		
N/A	22-04-2021	5	On Juniper Networks EX4300-MP Series, EX4600 Series, EX4650 Series, QFX5K Series deployed as a Virtual Chassis with a specific Layer 2 circuit configuration, Packet Forwarding Engine manager (FXPC) process may crash and restart upon receipt of specific layer 2 frames. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP Series, EX4600 Series, EX4650 Series, QFX5K Series 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4, 17.4R3-S5; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7,	https://kb.juniper.net/JS_A11132	H-JUN-EX46-040521/465

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2; CVE ID : CVE-2021-0237		
ex4650					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	4.3	A signal handler race condition exists in the Layer 2 Address Learning Daemon (L2ALD) of Juniper Networks Junos OS due to the absence of a specific protection mechanism to avoid a race condition which may allow an attacker to bypass the storm-control feature on devices. This issue is a corner case and only occurs during specific actions taken by an administrator of a device under certain specifics actions which triggers the event. The event occurs less frequently on devices which are not configured with Virtual Chassis configurations, and more frequently on devices configured in Virtual Chassis configurations. This issue is not specific to any particular Junos OS platform. An Indicator of Compromise (IoC) may be seen by reviewing log files	https://kb.juniper.net/JS_A11137	H-JUN-EX46-040521/466

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>for the following error message seen by executing the following show statement: show log messages grep storm Result to look for: /kernel: GENCFG: op 58 (Storm Control Blob) failed; err 1 (Unknown) This issue affects: Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D49 on EX Series; 15.1 versions prior to 15.1R7-S6; 15.1X49 versions prior to 15.1X49-D191, 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3; 17.2 versions prior to 17.2R2-S8, 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S5; 18.2 versions prior to 18.2R2-S6, 18.2R3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R1-S5, 18.4R2; 19.1 versions prior to 19.1R1-S4, 19.1R2.</p> <p>CVE ID : CVE-2021-0244</p>		
Improper Neutralization of Input During Web Page Generation ('Cross-site	22-04-2021	9.3	<p>A Cross-site Scripting (XSS) vulnerability in J-Web on Juniper Networks Junos OS allows an attacker to target another user's session thereby gaining access to the users session. The other</p>	https://kb.juniper.net/JS_A11166	H-JUN-EX46-040521/467

CVSS Scoring Scale	0-1	1-2	2-3	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')			<p>user session must be active for the attack to succeed. Once successful, the attacker has the same privileges as the user. If the user has root privileges, the attacker may be able to gain full control of the device. This issue affects: Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S15 on EX Series; 12.3X48 versions prior to 12.3X48-D95 on SRX Series; 15.1 versions prior to 15.1R7-S6 on EX Series; 15.1X49 versions prior to 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3; 19.1 versions prior to 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S3, 19.2R2; 19.3 versions prior to 19.3R2.</p> <p>CVE ID : CVE-2021-0275</p>		
N/A	22-04-2021	5	On Juniper Networks EX4300-MP Series, EX4600 Series, EX4650 Series,	https://kb.juniper.net/JS_A11132	H-JUN-EX46-040521/468

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>QFX5K Series deployed as a Virtual Chassis with a specific Layer 2 circuit configuration, Packet Forwarding Engine manager (FXPC) process may crash and restart upon receipt of specific layer 2 frames. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP Series, EX4600 Series, EX4650 Series, QFX5K Series 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4, 17.4R3-S5; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2;</p> <p>CVE ID : CVE-2021-0237</p>		
ex6210					
Double Free	22-04-2021	5	A Double Free vulnerability in the software forwarding interface daemon (sfid) process of Juniper	https://kb.juniper.net/JS_A11162	H-JUN-EX62-040521/469

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Networks Junos OS allows an adjacently-connected attacker to cause a Denial of Service (DoS) by sending a crafted ARP packet to the device. Continued receipt and processing of the crafted ARP packets will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX2200-C Series, EX3200 Series, EX3300 Series, EX4200 Series, EX4500 Series, EX4550 Series, EX6210 Series, EX8208 Series, EX8216 Series. 12.3 versions prior to 12.3R12-S17; 15.1 versions prior to 15.1R7-S8. This issue only affects the listed Marvell-chipset based EX Series devices. No other products or platforms are affected.</p> <p>CVE ID : CVE-2021-0271</p>		
ex8208					
Double Free	22-04-2021	5	<p>A Double Free vulnerability in the software forwarding interface daemon (sfid) process of Juniper Networks Junos OS allows an adjacently-connected attacker to cause a Denial of Service (DoS) by sending a crafted ARP packet to the device. Continued receipt and processing of the crafted ARP packets will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on</p>	https://kb.juniper.net/JS_A11162	H-JUN-EX82-040521/470

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EX2200-C Series, EX3200 Series, EX3300 Series, EX4200 Series, EX4500 Series, EX4550 Series, EX6210 Series, EX8208 Series, EX8216 Series. 12.3 versions prior to 12.3R12-S17; 15.1 versions prior to 15.1R7-S8. This issue only affects the listed Marvell-chipset based EX Series devices. No other products or platforms are affected. CVE ID : CVE-2021-0271		
ex8216					
Double Free	22-04-2021	5	A Double Free vulnerability in the software forwarding interface daemon (sfid) process of Juniper Networks Junos OS allows an adjacently-connected attacker to cause a Denial of Service (DoS) by sending a crafted ARP packet to the device. Continued receipt and processing of the crafted ARP packets will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX2200-C Series, EX3200 Series, EX3300 Series, EX4200 Series, EX4500 Series, EX4550 Series, EX6210 Series, EX8208 Series, EX8216 Series. 12.3 versions prior to 12.3R12-S17; 15.1 versions prior to 15.1R7-S8. This issue only affects the listed Marvell-chipset based EX Series devices. No other products	https://kb.juniper.net/JS_A11162	H-JUN-EX82-040521/471

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			or platforms are affected. CVE ID : CVE-2021-0271		
ex9200					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	4.3	A signal handler race condition exists in the Layer 2 Address Learning Daemon (L2ALD) of Juniper Networks Junos OS due to the absence of a specific protection mechanism to avoid a race condition which may allow an attacker to bypass the storm-control feature on devices. This issue is a corner case and only occurs during specific actions taken by an administrator of a device under certain specifics actions which triggers the event. The event occurs less frequently on devices which are not configured with Virtual Chassis configurations, and more frequently on devices configured in Virtual Chassis configurations. This issue is not specific to any particular Junos OS platform. An Indicator of Compromise (IoC) may be seen by reviewing log files for the following error message seen by executing the following show statement: show log messages grep storm Result to look for: /kernel: GENCFG: op 58 (Storm Control Blob) failed; err 1 (Unknown) This issue affects: Juniper Networks	https://kb.juniper.net/JS_A11137	H-JUN-EX92-040521/472

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Junos OS: 14.1X53 versions prior to 14.1X53-D49 on EX Series; 15.1 versions prior to 15.1R7-S6; 15.1X49 versions prior to 15.1X49-D191, 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3; 17.2 versions prior to 17.2R2-S8, 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S5; 18.2 versions prior to 18.2R2-S6, 18.2R3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R1-S5, 18.4R2; 19.1 versions prior to 19.1R1-S4, 19.1R2.</p> <p>CVE ID : CVE-2021-0244</p>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2021	9.3	<p>A Cross-site Scripting (XSS) vulnerability in J-Web on Juniper Networks Junos OS allows an attacker to target another user's session thereby gaining access to the users session. The other user session must be active for the attack to succeed. Once successful, the attacker has the same privileges as the user. If the user has root privileges, the attacker may be able to gain full control of the device. This issue affects: Juniper Networks Junos OS: 12.3</p>	https://kb.juniper.net/JS_A11166	H-JUN-EX92-040521/473

CVSS Scoring Scale	0-1	1-2	2-3	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 12.3R12-S15 on EX Series; 12.3X48 versions prior to 12.3X48-D95 on SRX Series; 15.1 versions prior to 15.1R7-S6 on EX Series; 15.1X49 versions prior to 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3; 19.1 versions prior to 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S3, 19.2R2; 19.3 versions prior to 19.3R2. CVE ID : CVE-2021-0275		
Uncontrolled Resource Consumption	22-04-2021	5	On Juniper Networks Junos OS platforms with link aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot	https://kb.juniper.net/JS_A11125	H-JUN-EX92-040521/474

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>might be required. The following log can be seen if this issue happens. /kernel: rt_pfe_veto: Memory over consumed. Op 1 err 12, rtsm_id 0:-1, msg type 72 /kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd</p> <p>An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<<</p> <p>user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<< This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000-72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3.</p> <p>CVE ID : CVE-2021-0230</p>		
ex9204					
Uncontrolled Resource Consumption	22-04-2021	5	<p>On Juniper Networks Junos OS platforms with link aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel: rt_pfe_veto: Memory over consumed. Op 1 err 12,</p>	https://kb.juniper.net/JS_A11125	H-JUN-EX92-040521/475

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>rtsm_id 0:-1, msg type 72 /kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device > show system virtual- memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<< user@device > show system virtual-memory no- forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<< This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000- 72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5;</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3.</p> <p>CVE ID : CVE-2021-0230</p>		
ex9208					
Uncontrolled Resource Consumption	22-04-2021	5	<p>On Juniper Networks Junos OS platforms with link aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel: rt_pfe_veto: Memory over consumed. Op 1 err 12, rtsm_id 0:-1, msg type 72 /kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd</p> <p>An administrator can use</p>	https://kb.juniper.net/JS_A11125	H-JUN-EX92-040521/476

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<<</p> <p>user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<< This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000-72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3. CVE ID : CVE-2021-0230		
ex9214					
Uncontrolled Resource Consumption	22-04-2021	5	On Juniper Networks Junos OS platforms with link aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel: rt_pfe_veto: Memory over consumed. Op 1 err 12, rtsm_id 0:-1, msg type 72 /kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device > show system virtual-	https://kb.juniper.net/JS_A11125	H-JUN-EX92-040521/477

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<< user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<< This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000-72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1;</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3. CVE ID : CVE-2021-0230		
ex9250					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	4.3	A signal handler race condition exists in the Layer 2 Address Learning Daemon (L2ALD) of Juniper Networks Junos OS due to the absence of a specific protection mechanism to avoid a race condition which may allow an attacker to bypass the storm-control feature on devices. This issue is a corner case and only occurs during specific actions taken by an administrator of a device under certain specifics actions which triggers the event. The event occurs less frequently on devices which are not configured with Virtual Chassis configurations, and more frequently on devices configured in Virtual Chassis configurations. This issue is not specific to any particular Junos OS platform. An Indicator of Compromise (IoC) may be seen by reviewing log files for the following error message seen by executing the following show	https://kb.juniper.net/JS_A11137	H-JUN-EX92-040521/478

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>statement: show log messages grep storm Result to look for: /kernel: GENCFG: op 58 (Storm Control Blob) failed; err 1 (Unknown) This issue affects: Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D49 on EX Series; 15.1 versions prior to 15.1R7-S6; 15.1X49 versions prior to 15.1X49-D191, 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3; 17.2 versions prior to 17.2R2-S8, 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S5; 18.2 versions prior to 18.2R2-S6, 18.2R3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R1-S5, 18.4R2; 19.1 versions prior to 19.1R1-S4, 19.1R2.</p> <p>CVE ID : CVE-2021-0244</p>		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2021	9.3	<p>A Cross-site Scripting (XSS) vulnerability in J-Web on Juniper Networks Junos OS allows an attacker to target another user's session thereby gaining access to the users session. The other user session must be active for the attack to succeed. Once successful, the</p>	https://kb.juniper.net/JS_A11166	H-JUN-EX92-040521/479

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker has the same privileges as the user. If the user has root privileges, the attacker may be able to gain full control of the device.</p> <p>This issue affects: Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S15 on EX Series; 12.3X48 versions prior to 12.3X48-D95 on SRX Series; 15.1 versions prior to 15.1R7-S6 on EX Series; 15.1X49 versions prior to 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3; 19.1 versions prior to 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S3, 19.2R2; 19.3 versions prior to 19.3R2.</p> <p>CVE ID : CVE-2021-0275</p>		
mx10					
NULL Pointer Dereference	22-04-2021	5	A NULL Pointer Dereference vulnerability in the Captive Portal Content Delivery (CPCD) services daemon (cpcd) of Juniper Networks	https://kb.juniper.net/JS_A11144	H-JUN-MX10-040521/480

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Junos OS on MX Series with MS-PIC, MS-SPC3, MS-MIC or MS-MPC allows an attacker to send malformed HTTP packets to the device thereby causing a Denial of Service (DoS), crashing the Multiservices PIC Management Daemon (mospmand) process thereby denying users the ability to login, while concurrently impacting other mospmand services and traffic through the device. Continued receipt and processing of these malformed packets will create a sustained Denial of Service (DoS) condition. While the Services PIC is restarting, all PIC services will be bypassed until the Services PIC completes its boot process. An attacker sending these malformed HTTP packets to the device who is not part of the Captive Portal experience is not able to exploit this issue. This issue is not applicable to MX RE-based CPCD platforms. This issue affects: Juniper Networks Junos OS on MX Series 17.3 version 17.3R1 and later versions prior to 17.4 versions 17.4R2-S9, 17.4R3-S2; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S3; 18.3 versions prior to 18.3R3-S1; 18.4 versions prior to 18.4R3; 19.1 versions prior</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R2; 19.3 versions prior to 19.3R3. This issue does not affect: Juniper Networks Junos OS versions prior to 17.3R1. CVE ID : CVE-2021-0251		
Uncontrolled Resource Consumption	22-04-2021	2.1	When a MX Series is configured as a Broadband Network Gateway (BNG) based on Layer 2 Tunneling Protocol (L2TP), executing certain CLI command may cause the system to run out of disk space, excessive disk usage may cause other complications. An administrator can use the following CLI command to monitor the available disk space: user@device> show system storage Filesystem Size Used Avail Capacity Mounted on /dev/gpt/junos 19G 18G 147M 99% /.mount <<<<< running out of space tmpfs 21G 16K 21G 0% /.mount/tmp tmpfs 5.3G 1.7M 5.3G 0% /.mount/mfs This issue affects Juniper Networks Junos OS on MX Series: 17.3R1 and later versions prior to 17.4R3-S5, 18.1 versions prior to 18.1R3-S13, 18.2 versions prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S7; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6,	https://kb.juniper.net/JS_A11133	H-JUN-MX10-040521/481

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2; 20.4 versions prior to 20.4R1-S1, 20.4R2; This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1. CVE ID : CVE-2021-0238		
Improper Check for Unusual or Exceptional Conditions	22-04-2021	5	An improper check for unusual or exceptional conditions vulnerability in Juniper Networks MX Series platforms with Trio-based MPC (Modular Port Concentrator) deployed in (Ethernet VPN) EVPN- (Virtual Extensible LAN) VXLAN configuration, may allow an attacker sending specific Layer 2 traffic to cause Distributed Denial of Service (DDoS) protection to trigger unexpectedly, resulting in traffic impact. Continued receipt and processing of this specific Layer 2 frames will sustain the Denial of Service (DoS) condition. An indication of compromise is to check DDOS LACP violations: user@device> show ddos-protection protocols statistics brief match lacp This issue only affects the MX Series platforms with Trio-based MPC. No other products or platforms are	https://kb.juniper.net/JS_A11123	H-JUN-MX10-040521/482

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>affected. This issue affects: Juniper Networks Junos OS on MX Series: 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S1, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2;</p> <p>CVE ID : CVE-2021-0228</p>		
Uncontrolled Resource Consumption	22-04-2021	5	<p>On Juniper Networks Junos OS platforms with link aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel: rt_pfe_veto: Memory over consumed. Op 1 err 12,</p>	https://kb.juniper.net/JS_A11125	H-JUN-MX10-040521/483

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
			<p>rtsm_id 0:-1, msg type 72 /kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device > show system virtual- memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<< user@device > show system virtual-memory no- forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<< This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000- 72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5;</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3.</p> <p>CVE ID : CVE-2021-0230</p>		
Improper Handling of Exceptional Conditions	22-04-2021	5	<p>A vulnerability in the processing of traffic matching a firewall filter containing a syslog action in Juniper Networks Junos OS on MX Series with MPC10/MPC11 cards installed, PTX10003 and PTX10008 Series devices, will cause the line card to crash and restart, creating a Denial of Service (DoS). Continued receipt and processing of packets matching the firewall filter can create a sustained Denial of Service (DoS) condition. When traffic hits the firewall filter, configured on lo0 or any physical interface on the line card, containing a term with a syslog action (e.g. 'term <name> then syslog'),</p>	<p>https://kb.juniper.net/JS_A11155, https://kb.juniper.net/TS_B17931</p>	H-JUN-MX10-040521/484

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>the affected line card will crash and restart, impacting traffic processing through the ports of the line card. This issue only affects MX Series routers with MPC10 or MPC11 line cards, and PTX10003 or PTX10008 Series packet transport routers. No other platforms or models of line cards are affected by this issue. Note: This issue has also been identified and described in technical service bulletin TSB17931 (login required). This issue affects: Juniper Networks Junos OS on MX Series: 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2. Juniper Networks Junos OS Evolved on PTX10003, PTX10008: All versions prior to 20.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1.</p> <p>CVE ID : CVE-2021-0264</p>		
mx10000					
Uncontrolled Resource Consumption	22-04-2021	2.1	<p>When a MX Series is configured as a Broadband Network Gateway (BNG) based on Layer 2 Tunneling Protocol (L2TP), executing certain CLI command may cause the system to run out</p>	https://kb.juniper.net/JS_A11133	H-JUN-MX10-040521/485

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>of disk space, excessive disk usage may cause other complications. An administrator can use the following CLI command to monitor the available disk space: user@device> show system storage Filesystem Size Used Avail Capacity Mounted on</p> <pre>/dev/gpt/junos 19G 18G 147M 99% /.mount <<<< running out of space tmpfs 21G 16K 21G 0% /.mount/tmp tmpfs 5.3G 1.7M 5.3G 0% /.mount/mfs</pre> <p>This issue affects Juniper Networks Junos OS on MX Series: 17.3R1 and later versions prior to 17.4R3-S5, 18.1 versions prior to 18.1R3-S13, 18.2 versions prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S7; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2; 20.4 versions prior to 20.4R1-S1, 20.4R2; This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1.</p> <p>CVE ID : CVE-2021-0238</p>		
Uncontrolled Resource	22-04-2021	5	On Juniper Networks Junos OS platforms with link	https://kb.juniper.net/JS	H-JUN-MX10-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Consumption			<p>aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel: rt_pfe_veto: Memory over consumed. Op 1 err 12, rtsm_id 0:-1, msg type 72 /kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd</p> <p>An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device</p> <pre>> show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<< user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<< This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000-</pre>	A11125	040521/486

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3.</p> <p>CVE ID : CVE-2021-0230</p>		
Improper Handling of Exceptional Conditions	22-04-2021	5	<p>A vulnerability in the processing of traffic matching a firewall filter containing a syslog action in Juniper Networks Junos OS on MX Series with MPC10/MPC11 cards installed, PTX10003 and</p>	<p>https://kb.juniper.net/JS_A11155, https://kb.juniper.net/TS_B17931</p>	H-JUN-MX10-040521/487

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>PTX10008 Series devices, will cause the line card to crash and restart, creating a Denial of Service (DoS). Continued receipt and processing of packets matching the firewall filter can create a sustained Denial of Service (DoS) condition. When traffic hits the firewall filter, configured on lo0 or any physical interface on the line card, containing a term with a syslog action (e.g. 'term <name> then syslog'), the affected line card will crash and restart, impacting traffic processing through the ports of the line card. This issue only affects MX Series routers with MPC10 or MPC11 line cards, and PTX10003 or PTX10008 Series packet transport routers. No other platforms or models of line cards are affected by this issue. Note: This issue has also been identified and described in technical service bulletin TSB17931 (login required). This issue affects: Juniper Networks Junos OS on MX Series: 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2. Juniper Networks Junos OS Evolved on</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PTX10003, PTX10008: All versions prior to 20.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1. CVE ID : CVE-2021-0264		
mx10003					
NULL Pointer Dereference	22-04-2021	5	A NULL Pointer Dereference vulnerability in the Captive Portal Content Delivery (CPCD) services daemon (cpcd) of Juniper Networks Junos OS on MX Series with MS-PIC, MS-SPC3, MS-MIC or MS-MPC allows an attacker to send malformed HTTP packets to the device thereby causing a Denial of Service (DoS), crashing the Multiservices PIC Management Daemon (mospmand) process thereby denying users the ability to login, while concurrently impacting other mospmand services and traffic through the device. Continued receipt and processing of these malformed packets will create a sustained Denial of Service (DoS) condition. While the Services PIC is restarting, all PIC services will be bypassed until the Services PIC completes its boot process. An attacker sending these malformed HTTP packets to the device who is not part of the Captive Portal experience is not able to exploit this	https://kb.juniper.net/JS_A11144	H-JUN-MX10-040521/488

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>issue. This issue is not applicable to MX RE-based CPCD platforms. This issue affects: Juniper Networks Junos OS on MX Series 17.3 version 17.3R1 and later versions prior to 17.4 versions 17.4R2-S9, 17.4R3-S2; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S3; 18.3 versions prior to 18.3R3-S1; 18.4 versions prior to 18.4R3; 19.1 versions prior to 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R2; 19.3 versions prior to 19.3R3. This issue does not affect: Juniper Networks Junos OS versions prior to 17.3R1.</p> <p>CVE ID : CVE-2021-0251</p>		
Uncontrolled Resource Consumption	22-04-2021	2.1	<p>When a MX Series is configured as a Broadband Network Gateway (BNG) based on Layer 2 Tunneling Protocol (L2TP), executing certain CLI command may cause the system to run out of disk space, excessive disk usage may cause other complications. An administrator can use the following CLI command to monitor the available disk space: user@device> show system storage Filesystem Size Used Avail Capacity Mounted on</p> <pre>/dev/gpt/junos 19G 18G 147M 99% /.mount <<<<< running out of space tmpfs 21G 16K 21G 0%</pre>	https://kb.juniper.net/JS_A11133	H-JUN-MX10-040521/489

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>/.mount/tmp tmpfs 5.3G 1.7M 5.3G 0% /.mount/mfs</p> <p>This issue affects Juniper Networks Junos OS on MX Series: 17.3R1 and later versions prior to 17.4R3-S5, 18.1 versions prior to 18.1R3-S13, 18.2 versions prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S7; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2; 20.4 versions prior to 20.4R1-S1, 20.4R2; This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1.</p> <p>CVE ID : CVE-2021-0238</p>		
Uncontrolled Resource Consumption	22-04-2021	5	<p>On Juniper Networks Junos OS platforms with link aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel:</p>	https://kb.juniper.net/JS_A11125	H-JUN-MX10-040521/490

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>rt_pfe_veto: Memory over consumed. Op 1 err 12, rtsm_id 0:-1, msg type 72 /kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd</p> <p>An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<<</p> <p>user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<< This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000-72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3.</p> <p>CVE ID : CVE-2021-0230</p>		
Improper Handling of Exceptional Conditions	22-04-2021	5	<p>A vulnerability in the processing of traffic matching a firewall filter containing a syslog action in Juniper Networks Junos OS on MX Series with MPC10/MPC11 cards installed, PTX10003 and PTX10008 Series devices, will cause the line card to crash and restart, creating a Denial of Service (DoS). Continued receipt and processing of packets matching the firewall filter can create a sustained Denial of Service (DoS) condition. When traffic hits the firewall filter, configured on lo0 or any physical interface on the line card, containing a term</p>	<p>https://kb.juniper.net/JS_A11155, https://kb.juniper.net/TS_B17931</p>	H-JUN-MX10-040521/491

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>with a syslog action (e.g. 'term <name> then syslog'), the affected line card will crash and restart, impacting traffic processing through the ports of the line card. This issue only affects MX Series routers with MPC10 or MPC11 line cards, and PTX10003 or PTX10008 Series packet transport routers. No other platforms or models of line cards are affected by this issue. Note: This issue has also been identified and described in technical service bulletin TSB17931 (login required). This issue affects: Juniper Networks Junos OS on MX Series: 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2. Juniper Networks Junos OS Evolved on PTX10003, PTX10008: All versions prior to 20.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1.</p> <p>CVE ID : CVE-2021-0264</p>		
mx10008					
NULL Pointer Dereference	22-04-2021	5	<p>A NULL Pointer Dereference vulnerability in the Captive Portal Content Delivery (CPCD) services daemon (cpcd) of Juniper Networks</p>	https://kb.juniper.net/JS_A11144	H-JUN-MX10-040521/492

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Junos OS on MX Series with MS-PIC, MS-SPC3, MS-MIC or MS-MPC allows an attacker to send malformed HTTP packets to the device thereby causing a Denial of Service (DoS), crashing the Multiservices PIC Management Daemon (mospmand) process thereby denying users the ability to login, while concurrently impacting other mospmand services and traffic through the device. Continued receipt and processing of these malformed packets will create a sustained Denial of Service (DoS) condition. While the Services PIC is restarting, all PIC services will be bypassed until the Services PIC completes its boot process. An attacker sending these malformed HTTP packets to the device who is not part of the Captive Portal experience is not able to exploit this issue. This issue is not applicable to MX RE-based CPCD platforms. This issue affects: Juniper Networks Junos OS on MX Series 17.3 version 17.3R1 and later versions prior to 17.4 versions 17.4R2-S9, 17.4R3-S2; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S3; 18.3 versions prior to 18.3R3-S1; 18.4 versions prior to 18.4R3; 19.1 versions prior</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R2; 19.3 versions prior to 19.3R3. This issue does not affect: Juniper Networks Junos OS versions prior to 17.3R1. CVE ID : CVE-2021-0251		
Improper Handling of Exceptional Conditions	22-04-2021	5	A vulnerability in the processing of traffic matching a firewall filter containing a syslog action in Juniper Networks Junos OS on MX Series with MPC10/MPC11 cards installed, PTX10003 and PTX10008 Series devices, will cause the line card to crash and restart, creating a Denial of Service (DoS). Continued receipt and processing of packets matching the firewall filter can create a sustained Denial of Service (DoS) condition. When traffic hits the firewall filter, configured on lo0 or any physical interface on the line card, containing a term with a syslog action (e.g. 'term <name> then syslog'), the affected line card will crash and restart, impacting traffic processing through the ports of the line card. This issue only affects MX Series routers with MPC10 or MPC11 line cards, and PTX10003 or PTX10008 Series packet transport routers. No other platforms or models of line cards are	https://kb.juniper.net/JS_A11155 , https://kb.juniper.net/TS_B17931	H-JUN-MX10-040521/493

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>affected by this issue. Note: This issue has also been identified and described in technical service bulletin TSB17931 (login required). This issue affects: Juniper Networks Junos OS on MX Series: 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2. Juniper Networks Junos OS Evolved on PTX10003, PTX10008: All versions prior to 20.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1.</p> <p>CVE ID : CVE-2021-0264</p>		
mx10016					
NULL Pointer Dereference	22-04-2021	5	<p>A NULL Pointer Dereference vulnerability in the Captive Portal Content Delivery (CPCD) services daemon (cpd) of Juniper Networks Junos OS on MX Series with MS-PIC, MS-SPC3, MS-MIC or MS-MPC allows an attacker to send malformed HTTP packets to the device thereby causing a Denial of Service (DoS), crashing the Multiservices PIC Management Daemon (mspmnd) process thereby denying users the ability to login, while concurrently impacting other mspmand</p>	https://kb.juniper.net/JS_A11144	H-JUN-MX10-040521/494

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>services and traffic through the device. Continued receipt and processing of these malformed packets will create a sustained Denial of Service (DoS) condition. While the Services PIC is restarting, all PIC services will be bypassed until the Services PIC completes its boot process. An attacker sending these malformed HTTP packets to the device who is not part of the Captive Portal experience is not able to exploit this issue. This issue is not applicable to MX RE-based CPCD platforms. This issue affects: Juniper Networks Junos OS on MX Series 17.3 version 17.3R1 and later versions prior to 17.4 versions 17.4R2-S9, 17.4R3-S2; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S3; 18.3 versions prior to 18.3R3-S1; 18.4 versions prior to 18.4R3; 19.1 versions prior to 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R2; 19.3 versions prior to 19.3R3. This issue does not affect: Juniper Networks Junos OS versions prior to 17.3R1.</p> <p>CVE ID : CVE-2021-0251</p>		
Improper Handling of Exceptional Conditions	22-04-2021	5	<p>A vulnerability in the processing of traffic matching a firewall filter containing a syslog action in</p>	https://kb.juniper.net/JS_A11155 , https://kb.juniper.net/JS_A11155	H-JUN-MX10-040521/495

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Juniper Networks Junos OS on MX Series with MPC10/MPC11 cards installed, PTX10003 and PTX10008 Series devices, will cause the line card to crash and restart, creating a Denial of Service (DoS). Continued receipt and processing of packets matching the firewall filter can create a sustained Denial of Service (DoS) condition. When traffic hits the firewall filter, configured on lo0 or any physical interface on the line card, containing a term with a syslog action (e.g. 'term <name> then syslog'), the affected line card will crash and restart, impacting traffic processing through the ports of the line card. This issue only affects MX Series routers with MPC10 or MPC11 line cards, and PTX10003 or PTX10008 Series packet transport routers. No other platforms or models of line cards are affected by this issue. Note: This issue has also been identified and described in technical service bulletin TSB17931 (login required). This issue affects: Juniper Networks Junos OS on MX Series: 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3</p>	niper.net/TSB17931	

CVSS Scoring Scale	0-1	1-2	2-3	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 20.3R3; 20.4 versions prior to 20.4R2. Juniper Networks Junos OS Evolved on PTX10003, PTX10008: All versions prior to 20.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1. CVE ID : CVE-2021-0264		
mx104					
NULL Pointer Dereference	22-04-2021	5	A NULL Pointer Dereference vulnerability in the Captive Portal Content Delivery (CPCD) services daemon (cpcd) of Juniper Networks Junos OS on MX Series with MS-PIC, MS-SPC3, MS-MIC or MS-MPC allows an attacker to send malformed HTTP packets to the device thereby causing a Denial of Service (DoS), crashing the Multiservices PIC Management Daemon (mispmand) process thereby denying users the ability to login, while concurrently impacting other mispmand services and traffic through the device. Continued receipt and processing of these malformed packets will create a sustained Denial of Service (DoS) condition. While the Services PIC is restarting, all PIC services will be bypassed until the Services PIC completes its boot process. An attacker sending these malformed	https://kb.juniper.net/JS_A11144	H-JUN-MX10-040521/496

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>HTTP packets to the device who is not part of the Captive Portal experience is not able to exploit this issue. This issue is not applicable to MX RE-based CPCD platforms. This issue affects: Juniper Networks Junos OS on MX Series 17.3 version 17.3R1 and later versions prior to 17.4 versions 17.4R2-S9, 17.4R3-S2; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S3; 18.3 versions prior to 18.3R3-S1; 18.4 versions prior to 18.4R3; 19.1 versions prior to 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R2; 19.3 versions prior to 19.3R3. This issue does not affect: Juniper Networks Junos OS versions prior to 17.3R1.</p> <p>CVE ID : CVE-2021-0251</p>		
Uncontrolled Resource Consumption	22-04-2021	2.1	<p>When a MX Series is configured as a Broadband Network Gateway (BNG) based on Layer 2 Tunneling Protocol (L2TP), executing certain CLI command may cause the system to run out of disk space, excessive disk usage may cause other complications. An administrator can use the following CLI command to monitor the available disk space: user@device> show system storage Filesystem Size Used Avail Capacity Mounted on</p>	https://kb.juniper.net/JS_A11133	H-JUN-MX10-040521/497

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			/dev/gpt/junos 19G 18G 147M 99% /.mount <<<<< running out of space tmpfs 21G 16K 21G 0% /.mount/tmp tmpfs 5.3G 1.7M 5.3G 0% /.mount/mfs This issue affects Juniper Networks Junos OS on MX Series: 17.3R1 and later versions prior to 17.4R3-S5, 18.1 versions prior to 18.1R3-S13, 18.2 versions prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S7; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2; 20.4 versions prior to 20.4R1-S1, 20.4R2; This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1. CVE ID : CVE-2021-0238		
Improper Check for Unusual or Exceptional Conditions	22-04-2021	5	An improper check for unusual or exceptional conditions vulnerability in Juniper Networks MX Series platforms with Trio-based MPC (Modular Port Concentrator) deployed in (Ethernet VPN) EVPN- (Virtual Extensible LAN) VXLAN configuration, may allow an attacker sending specific Layer 2 traffic to	https://kb.juniper.net/JS_A11123	H-JUN-MX10-040521/498

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>cause Distributed Denial of Service (DDoS) protection to trigger unexpectedly, resulting in traffic impact. Continued receipt and processing of this specific Layer 2 frames will sustain the Denial of Service (DoS) condition. An indication of compromise is to check DDOS LACP violations: user@device> show ddos-protection protocols statistics brief match lacp</p> <p>This issue only affects the MX Series platforms with Trio-based MPC. No other products or platforms are affected. This issue affects: Juniper Networks Junos OS on MX Series: 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S1, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2;</p> <p>CVE ID : CVE-2021-0228</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	22-04-2021	5	<p>On Juniper Networks Junos OS platforms with link aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel: rt_pfe_veto: Memory over consumed. Op 1 err 12, rtsm_id 0:-1, msg type 72 /kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd</p> <p>An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<<</p> <p>user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<< This issue does not affect the following platforms: Juniper</p>	https://kb.juniper.net/JS_A11125	H-JUN-MX10-040521/499

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Networks MX Series. Juniper Networks PTX1000-72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3.</p> <p>CVE ID : CVE-2021-0230</p>		
Improper Handling of Exceptional Conditions	22-04-2021	5	<p>A vulnerability in the processing of traffic matching a firewall filter containing a syslog action in Juniper Networks Junos OS on MX Series with</p>	https://kb.juniper.net/JS_A11155 , https://kb.juniper.net/TS_B17931	H-JUN-MX10-040521/500

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>MPC10/MPC11 cards installed, PTX10003 and PTX10008 Series devices, will cause the line card to crash and restart, creating a Denial of Service (DoS). Continued receipt and processing of packets matching the firewall filter can create a sustained Denial of Service (DoS) condition. When traffic hits the firewall filter, configured on lo0 or any physical interface on the line card, containing a term with a syslog action (e.g. 'term <name> then syslog'), the affected line card will crash and restart, impacting traffic processing through the ports of the line card. This issue only affects MX Series routers with MPC10 or MPC11 line cards, and PTX10003 or PTX10008 Series packet transport routers. No other platforms or models of line cards are affected by this issue. Note: This issue has also been identified and described in technical service bulletin TSB17931 (login required). This issue affects: Juniper Networks Junos OS on MX Series: 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R3; 20.4 versions prior to</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.4R2. Juniper Networks Junos OS Evolved on PTX10003, PTX10008: All versions prior to 20.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1. CVE ID : CVE-2021-0264		
mx150					
NULL Pointer Dereference	22-04-2021	5	A NULL Pointer Dereference vulnerability in the Captive Portal Content Delivery (CPCD) services daemon (cpcd) of Juniper Networks Junos OS on MX Series with MS-PIC, MS-SPC3, MS-MIC or MS-MPC allows an attacker to send malformed HTTP packets to the device thereby causing a Denial of Service (DoS), crashing the Multiservices PIC Management Daemon (mspmmand) process thereby denying users the ability to login, while concurrently impacting other mspmand services and traffic through the device. Continued receipt and processing of these malformed packets will create a sustained Denial of Service (DoS) condition. While the Services PIC is restarting, all PIC services will be bypassed until the Services PIC completes its boot process. An attacker sending these malformed HTTP packets to the device who is not part of the	https://kb.juniper.net/JS_A11144	H-JUN-MX15-040521/501

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Captive Portal experience is not able to exploit this issue. This issue is not applicable to MX RE-based CPCD platforms. This issue affects: Juniper Networks Junos OS on MX Series 17.3 version 17.3R1 and later versions prior to 17.4 versions 17.4R2-S9, 17.4R3-S2; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S3; 18.3 versions prior to 18.3R3-S1; 18.4 versions prior to 18.4R3; 19.1 versions prior to 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R2; 19.3 versions prior to 19.3R3. This issue does not affect: Juniper Networks Junos OS versions prior to 17.3R1.</p> <p>CVE ID : CVE-2021-0251</p>		
Uncontrolled Resource Consumption	22-04-2021	2.1	<p>When a MX Series is configured as a Broadband Network Gateway (BNG) based on Layer 2 Tunneling Protocol (L2TP), executing certain CLI command may cause the system to run out of disk space, excessive disk usage may cause other complications. An administrator can use the following CLI command to monitor the available disk space: user@device> show system storage Filesystem Size Used Avail Capacity Mounted on</p> <p>/dev/gpt/junos 19G 18G 147M 99% /.mount <<<<<</p>	https://kb.juniper.net/JS_A11133	H-JUN-MX15-040521/502

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>running out of space tmpfs 21G 16K 21G 0% /.mount/tmp tmpfs 5.3G 1.7M 5.3G 0% /.mount/mfs This issue affects Juniper Networks Junos OS on MX Series: 17.3R1 and later versions prior to 17.4R3-S5, 18.1 versions prior to 18.1R3-S13, 18.2 versions prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S7; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2; 20.4 versions prior to 20.4R1-S1, 20.4R2; This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1.</p> <p>CVE ID : CVE-2021-0238</p>		
Improper Check for Unusual or Exceptional Conditions	22-04-2021	5	<p>An improper check for unusual or exceptional conditions vulnerability in Juniper Networks MX Series platforms with Trio-based MPC (Modular Port Concentrator) deployed in (Ethernet VPN) EVPN- (Virtual Extensible LAN) VXLAN configuration, may allow an attacker sending specific Layer 2 traffic to cause Distributed Denial of Service (DDoS) protection</p>	https://kb.juniper.net/JS_A11123	H-JUN-MX15-040521/503

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>to trigger unexpectedly, resulting in traffic impact. Continued receipt and processing of this specific Layer 2 frames will sustain the Denial of Service (DoS) condition. An indication of compromise is to check DDOS LACP violations: user@device> show ddos-protection protocols statistics brief match lacp</p> <p>This issue only affects the MX Series platforms with Trio-based MPC. No other products or platforms are affected. This issue affects: Juniper Networks Junos OS on MX Series: 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S1, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2;</p> <p>CVE ID : CVE-2021-0228</p>		
Uncontrolled Resource	22-04-2021	5	On Juniper Networks Junos OS platforms with link	https://kb.juniper.net/JS	H-JUN-MX15-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Consumption			<p>aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel: rt_pfe_veto: Memory over consumed. Op 1 err 12, rtsm_id 0:-1, msg type 72 /kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd</p> <p>An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device</p> <pre>> show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<< user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<< This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000-</pre>	A11125	040521/504

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3.</p> <p>CVE ID : CVE-2021-0230</p>		
Improper Handling of Exceptional Conditions	22-04-2021	5	<p>A vulnerability in the processing of traffic matching a firewall filter containing a syslog action in Juniper Networks Junos OS on MX Series with MPC10/MPC11 cards installed, PTX10003 and</p>	<p>https://kb.juniper.net/JS_A11155, https://kb.juniper.net/TS_B17931</p>	H-JUN-MX15-040521/505

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>PTX10008 Series devices, will cause the line card to crash and restart, creating a Denial of Service (DoS). Continued receipt and processing of packets matching the firewall filter can create a sustained Denial of Service (DoS) condition. When traffic hits the firewall filter, configured on lo0 or any physical interface on the line card, containing a term with a syslog action (e.g. 'term <name> then syslog'), the affected line card will crash and restart, impacting traffic processing through the ports of the line card. This issue only affects MX Series routers with MPC10 or MPC11 line cards, and PTX10003 or PTX10008 Series packet transport routers. No other platforms or models of line cards are affected by this issue. Note: This issue has also been identified and described in technical service bulletin TSB17931 (login required). This issue affects: Juniper Networks Junos OS on MX Series: 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2. Juniper Networks Junos OS Evolved on</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PTX10003, PTX10008: All versions prior to 20.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1. CVE ID : CVE-2021-0264		
mx2008					
NULL Pointer Dereference	22-04-2021	5	A NULL Pointer Dereference vulnerability in the Captive Portal Content Delivery (CPCD) services daemon (cpcd) of Juniper Networks Junos OS on MX Series with MS-PIC, MS-SPC3, MS-MIC or MS-MPC allows an attacker to send malformed HTTP packets to the device thereby causing a Denial of Service (DoS), crashing the Multiservices PIC Management Daemon (mospmand) process thereby denying users the ability to login, while concurrently impacting other mospmand services and traffic through the device. Continued receipt and processing of these malformed packets will create a sustained Denial of Service (DoS) condition. While the Services PIC is restarting, all PIC services will be bypassed until the Services PIC completes its boot process. An attacker sending these malformed HTTP packets to the device who is not part of the Captive Portal experience is not able to exploit this	https://kb.juniper.net/JS_A11144	H-JUN-MX20-040521/506

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>issue. This issue is not applicable to MX RE-based CPCD platforms. This issue affects: Juniper Networks Junos OS on MX Series 17.3 version 17.3R1 and later versions prior to 17.4 versions 17.4R2-S9, 17.4R3-S2; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S3; 18.3 versions prior to 18.3R3-S1; 18.4 versions prior to 18.4R3; 19.1 versions prior to 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R2; 19.3 versions prior to 19.3R3. This issue does not affect: Juniper Networks Junos OS versions prior to 17.3R1.</p> <p>CVE ID : CVE-2021-0251</p>		
Uncontrolled Resource Consumption	22-04-2021	2.1	<p>When a MX Series is configured as a Broadband Network Gateway (BNG) based on Layer 2 Tunneling Protocol (L2TP), executing certain CLI command may cause the system to run out of disk space, excessive disk usage may cause other complications. An administrator can use the following CLI command to monitor the available disk space: user@device> show system storage Filesystem Size Used Avail Capacity Mounted on</p> <pre>/dev/gpt/junos 19G 18G 147M 99% /.mount <<<<< running out of space tmpfs 21G 16K 21G 0%</pre>	https://kb.juniper.net/JS_A11133	H-JUN-MX20-040521/507

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>/.mount/tmp tmpfs 5.3G 1.7M 5.3G 0% /.mount/mfs</p> <p>This issue affects Juniper Networks Junos OS on MX Series: 17.3R1 and later versions prior to 17.4R3-S5, 18.1 versions prior to 18.1R3-S13, 18.2 versions prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S7; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2; 20.4 versions prior to 20.4R1-S1, 20.4R2; This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1.</p> <p>CVE ID : CVE-2021-0238</p>		
Uncontrolled Resource Consumption	22-04-2021	5	<p>On Juniper Networks Junos OS platforms with link aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel:</p>	https://kb.juniper.net/JS_A11125	H-JUN-MX20-040521/508

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>rt_pfe_veto: Memory over consumed. Op 1 err 12, rtsm_id 0:-1, msg type 72 /kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd</p> <p>An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<<</p> <p>user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<< This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000-72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3.</p> <p>CVE ID : CVE-2021-0230</p>		
Improper Handling of Exceptional Conditions	22-04-2021	5	<p>A vulnerability in the processing of traffic matching a firewall filter containing a syslog action in Juniper Networks Junos OS on MX Series with MPC10/MPC11 cards installed, PTX10003 and PTX10008 Series devices, will cause the line card to crash and restart, creating a Denial of Service (DoS). Continued receipt and processing of packets matching the firewall filter can create a sustained Denial of Service (DoS) condition. When traffic hits the firewall filter, configured on lo0 or any physical interface on the line card, containing a term</p>	<p>https://kb.juniper.net/JS_A11155, https://kb.juniper.net/TS_B17931</p>	H-JUN-MX20-040521/509

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>with a syslog action (e.g. 'term <name> then syslog'), the affected line card will crash and restart, impacting traffic processing through the ports of the line card. This issue only affects MX Series routers with MPC10 or MPC11 line cards, and PTX10003 or PTX10008 Series packet transport routers. No other platforms or models of line cards are affected by this issue. Note: This issue has also been identified and described in technical service bulletin TSB17931 (login required). This issue affects: Juniper Networks Junos OS on MX Series: 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2. Juniper Networks Junos OS Evolved on PTX10003, PTX10008: All versions prior to 20.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1.</p> <p>CVE ID : CVE-2021-0264</p>		
mx2010					
NULL Pointer Dereference	22-04-2021	5	<p>A NULL Pointer Dereference vulnerability in the Captive Portal Content Delivery (CPCD) services daemon (cpcd) of Juniper Networks</p>	https://kb.juniper.net/JS_A11144	H-JUN-MX20-040521/510

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Junos OS on MX Series with MS-PIC, MS-SPC3, MS-MIC or MS-MPC allows an attacker to send malformed HTTP packets to the device thereby causing a Denial of Service (DoS), crashing the Multiservices PIC Management Daemon (mspmmand) process thereby denying users the ability to login, while concurrently impacting other mspmand services and traffic through the device. Continued receipt and processing of these malformed packets will create a sustained Denial of Service (DoS) condition. While the Services PIC is restarting, all PIC services will be bypassed until the Services PIC completes its boot process. An attacker sending these malformed HTTP packets to the device who is not part of the Captive Portal experience is not able to exploit this issue. This issue is not applicable to MX RE-based CPCD platforms. This issue affects: Juniper Networks Junos OS on MX Series 17.3 version 17.3R1 and later versions prior to 17.4 versions 17.4R2-S9, 17.4R3-S2; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S3; 18.3 versions prior to 18.3R3-S1; 18.4 versions prior to 18.4R3; 19.1 versions prior</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R2; 19.3 versions prior to 19.3R3. This issue does not affect: Juniper Networks Junos OS versions prior to 17.3R1. CVE ID : CVE-2021-0251		
Uncontrolled Resource Consumption	22-04-2021	2.1	When a MX Series is configured as a Broadband Network Gateway (BNG) based on Layer 2 Tunneling Protocol (L2TP), executing certain CLI command may cause the system to run out of disk space, excessive disk usage may cause other complications. An administrator can use the following CLI command to monitor the available disk space: user@device> show system storage Filesystem Size Used Avail Capacity Mounted on /dev/gpt/junos 19G 18G 147M 99% /.mount <<<<< running out of space tmpfs 21G 16K 21G 0% /.mount/tmp tmpfs 5.3G 1.7M 5.3G 0% /.mount/mfs This issue affects Juniper Networks Junos OS on MX Series: 17.3R1 and later versions prior to 17.4R3-S5, 18.1 versions prior to 18.1R3-S13, 18.2 versions prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S7; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6,	https://kb.juniper.net/JS_A11133	H-JUN-MX20-040521/511

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2; 20.4 versions prior to 20.4R1-S1, 20.4R2; This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1. CVE ID : CVE-2021-0238		
Uncontrolled Resource Consumption	22-04-2021	5	On Juniper Networks Junos OS platforms with link aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel: rt_pfe_veto: Memory over consumed. Op 1 err 12, rtsm_id 0:-1, msg type 72 /kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device > show system virtual-memory no-forwarding match ifstat Type InUse	https://kb.juniper.net/JS_A11125	H-JUN-MX20-040521/512

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<< user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<< This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000-72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2</p>		

CVSS Scoring Scale	0-1	1-2	2-3	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 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3. CVE ID : CVE-2021-0230		
Improper Handling of Exceptional Conditions	22-04-2021	5	A vulnerability in the processing of traffic matching a firewall filter containing a syslog action in Juniper Networks Junos OS on MX Series with MPC10/MPC11 cards installed, PTX10003 and PTX10008 Series devices, will cause the line card to crash and restart, creating a Denial of Service (DoS). Continued receipt and processing of packets matching the firewall filter can create a sustained Denial of Service (DoS) condition. When traffic hits the firewall filter, configured on lo0 or any physical interface on the line card, containing a term with a syslog action (e.g. 'term <name> then syslog'), the affected line card will crash and restart, impacting traffic processing through the ports of the line card. This issue only affects MX Series routers with MPC10 or MPC11 line cards, and PTX10003 or PTX10008 Series packet transport routers. No other platforms or models of line cards are affected by this issue. Note:	https://kb.juniper.net/JS_A11155 , https://kb.juniper.net/TS_B17931	H-JUN-MX20-040521/513

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>This issue has also been identified and described in technical service bulletin TSB17931 (login required). This issue affects: Juniper Networks Junos OS on MX Series: 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2. Juniper Networks Junos OS Evolved on PTX10003, PTX10008: All versions prior to 20.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1.</p> <p>CVE ID : CVE-2021-0264</p>		

mx2020

NULL Pointer Dereference	22-04-2021	5	<p>A NULL Pointer Dereference vulnerability in the Captive Portal Content Delivery (CPCD) services daemon (cpd) of Juniper Networks Junos OS on MX Series with MS-PIC, MS-SPC3, MS-MIC or MS-MPC allows an attacker to send malformed HTTP packets to the device thereby causing a Denial of Service (DoS), crashing the Multiservices PIC Management Daemon (mspmnd) process thereby denying users the ability to login, while concurrently impacting other mspmand services and traffic through</p>	https://kb.juniper.net/JS_A11144	H-JUN-MX20-040521/514
--------------------------	------------	---	---	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>the device. Continued receipt and processing of these malformed packets will create a sustained Denial of Service (DoS) condition. While the Services PIC is restarting, all PIC services will be bypassed until the Services PIC completes its boot process. An attacker sending these malformed HTTP packets to the device who is not part of the Captive Portal experience is not able to exploit this issue. This issue is not applicable to MX RE-based CPCD platforms. This issue affects: Juniper Networks Junos OS on MX Series 17.3 version 17.3R1 and later versions prior to 17.4 versions 17.4R2-S9, 17.4R3-S2; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S3; 18.3 versions prior to 18.3R3-S1; 18.4 versions prior to 18.4R3; 19.1 versions prior to 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R2; 19.3 versions prior to 19.3R3. This issue does not affect: Juniper Networks Junos OS versions prior to 17.3R1.</p> <p>CVE ID : CVE-2021-0251</p>		
Uncontrolled Resource Consumption	22-04-2021	2.1	<p>When a MX Series is configured as a Broadband Network Gateway (BNG) based on Layer 2 Tunneling Protocol (L2TP), executing</p>	https://kb.juniper.net/JS_A11133	H-JUN-MX20-040521/515

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>certain CLI command may cause the system to run out of disk space, excessive disk usage may cause other complications. An administrator can use the following CLI command to monitor the available disk space: user@device> show system storage Filesystem Size Used Avail Capacity Mounted on</p> <pre>/dev/gpt/junos 19G 18G 147M 99% /.mount <<<<< running out of space tmpfs 21G 16K 21G 0% /.mount/tmp tmpfs 5.3G 1.7M 5.3G 0% /.mount/mfs</pre> <p>This issue affects Juniper Networks Junos OS on MX Series: 17.3R1 and later versions prior to 17.4R3-S5, 18.1 versions prior to 18.1R3-S13, 18.2 versions prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S7; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2; 20.4 versions prior to 20.4R1-S1, 20.4R2; This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1.</p> <p>CVE ID : CVE-2021-0238</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	22-04-2021	5	<p>On Juniper Networks Junos OS platforms with link aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel: rt_pfe_veto: Memory over consumed. Op 1 err 12, rtsm_id 0:-1, msg type 72 /kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd</p> <p>An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<<</p> <p>user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<< This issue does not affect the following platforms: Juniper</p>	https://kb.juniper.net/JS_A11125	H-JUN-MX20-040521/516

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Networks MX Series. Juniper Networks PTX1000-72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3.</p> <p>CVE ID : CVE-2021-0230</p>		
Improper Handling of Exceptional Conditions	22-04-2021	5	<p>A vulnerability in the processing of traffic matching a firewall filter containing a syslog action in Juniper Networks Junos OS on MX Series with</p>	https://kb.juniper.net/JS_A11155 , https://kb.juniper.net/TS_B17931	H-JUN-MX20-040521/517

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>MPC10/MPC11 cards installed, PTX10003 and PTX10008 Series devices, will cause the line card to crash and restart, creating a Denial of Service (DoS). Continued receipt and processing of packets matching the firewall filter can create a sustained Denial of Service (DoS) condition. When traffic hits the firewall filter, configured on lo0 or any physical interface on the line card, containing a term with a syslog action (e.g. 'term <name> then syslog'), the affected line card will crash and restart, impacting traffic processing through the ports of the line card. This issue only affects MX Series routers with MPC10 or MPC11 line cards, and PTX10003 or PTX10008 Series packet transport routers. No other platforms or models of line cards are affected by this issue. Note: This issue has also been identified and described in technical service bulletin TSB17931 (login required). This issue affects: Juniper Networks Junos OS on MX Series: 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R3; 20.4 versions prior to</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.4R2. Juniper Networks Junos OS Evolved on PTX10003, PTX10008: All versions prior to 20.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1. CVE ID : CVE-2021-0264		
mx204					
NULL Pointer Dereference	22-04-2021	5	A NULL Pointer Dereference vulnerability in the Captive Portal Content Delivery (CPCD) services daemon (cpcd) of Juniper Networks Junos OS on MX Series with MS-PIC, MS-SPC3, MS-MIC or MS-MPC allows an attacker to send malformed HTTP packets to the device thereby causing a Denial of Service (DoS), crashing the Multiservices PIC Management Daemon (mospmand) process thereby denying users the ability to login, while concurrently impacting other mospmand services and traffic through the device. Continued receipt and processing of these malformed packets will create a sustained Denial of Service (DoS) condition. While the Services PIC is restarting, all PIC services will be bypassed until the Services PIC completes its boot process. An attacker sending these malformed HTTP packets to the device who is not part of the	https://kb.juniper.net/JS_A11144	H-JUN-MX20-040521/518

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Captive Portal experience is not able to exploit this issue. This issue is not applicable to MX RE-based CPCD platforms. This issue affects: Juniper Networks Junos OS on MX Series 17.3 version 17.3R1 and later versions prior to 17.4 versions 17.4R2-S9, 17.4R3-S2; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S3; 18.3 versions prior to 18.3R3-S1; 18.4 versions prior to 18.4R3; 19.1 versions prior to 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R2; 19.3 versions prior to 19.3R3. This issue does not affect: Juniper Networks Junos OS versions prior to 17.3R1.</p> <p>CVE ID : CVE-2021-0251</p>		
Uncontrolled Resource Consumption	22-04-2021	2.1	<p>When a MX Series is configured as a Broadband Network Gateway (BNG) based on Layer 2 Tunneling Protocol (L2TP), executing certain CLI command may cause the system to run out of disk space, excessive disk usage may cause other complications. An administrator can use the following CLI command to monitor the available disk space: user@device> show system storage Filesystem Size Used Avail Capacity Mounted on</p> <p>/dev/gpt/junos 19G 18G 147M 99% /.mount <<<<<</p>	https://kb.juniper.net/JS_A11133	H-JUN-MX20-040521/519

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>running out of space tmpfs 21G 16K 21G 0% /.mount/tmp tmpfs 5.3G 1.7M 5.3G 0% /.mount/mfs This issue affects Juniper Networks Junos OS on MX Series: 17.3R1 and later versions prior to 17.4R3-S5, 18.1 versions prior to 18.1R3-S13, 18.2 versions prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S7; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2; 20.4 versions prior to 20.4R1-S1, 20.4R2; This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1.</p> <p>CVE ID : CVE-2021-0238</p>		
Improper Check for Unusual or Exceptional Conditions	22-04-2021	5	<p>An improper check for unusual or exceptional conditions vulnerability in Juniper Networks MX Series platforms with Trio-based MPC (Modular Port Concentrator) deployed in (Ethernet VPN) EVPN- (Virtual Extensible LAN) VXLAN configuration, may allow an attacker sending specific Layer 2 traffic to cause Distributed Denial of Service (DDoS) protection</p>	https://kb.juniper.net/JS_A11123	H-JUN-MX20-040521/520

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
			<p>to trigger unexpectedly, resulting in traffic impact. Continued receipt and processing of this specific Layer 2 frames will sustain the Denial of Service (DoS) condition. An indication of compromise is to check DDOS LACP violations: user@device> show ddos-protection protocols statistics brief match lacp</p> <p>This issue only affects the MX Series platforms with Trio-based MPC. No other products or platforms are affected. This issue affects: Juniper Networks Junos OS on MX Series: 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S1, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2;</p> <p>CVE ID : CVE-2021-0228</p>		
Uncontrolled Resource	22-04-2021	5	On Juniper Networks Junos OS platforms with link	https://kb.juniper.net/JS	H-JUN-MX20-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Consumption			<p>aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel: rt_pfe_veto: Memory over consumed. Op 1 err 12, rtsm_id 0:-1, msg type 72 /kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd</p> <p>An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device</p> <pre>> show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<< user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<< This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000-</pre>	A11125	040521/521

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3.</p> <p>CVE ID : CVE-2021-0230</p>		
Improper Handling of Exceptional Conditions	22-04-2021	5	<p>A vulnerability in the processing of traffic matching a firewall filter containing a syslog action in Juniper Networks Junos OS on MX Series with MPC10/MPC11 cards installed, PTX10003 and</p>	<p>https://kb.juniper.net/JS_A11155, https://kb.juniper.net/TS_B17931</p>	H-JUN-MX20-040521/522

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>PTX10008 Series devices, will cause the line card to crash and restart, creating a Denial of Service (DoS). Continued receipt and processing of packets matching the firewall filter can create a sustained Denial of Service (DoS) condition. When traffic hits the firewall filter, configured on lo0 or any physical interface on the line card, containing a term with a syslog action (e.g. 'term <name> then syslog'), the affected line card will crash and restart, impacting traffic processing through the ports of the line card. This issue only affects MX Series routers with MPC10 or MPC11 line cards, and PTX10003 or PTX10008 Series packet transport routers. No other platforms or models of line cards are affected by this issue. Note: This issue has also been identified and described in technical service bulletin TSB17931 (login required). This issue affects: Juniper Networks Junos OS on MX Series: 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2. Juniper Networks Junos OS Evolved on</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PTX10003, PTX10008: All versions prior to 20.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1. CVE ID : CVE-2021-0264		
mx240					
NULL Pointer Dereference	22-04-2021	5	A NULL Pointer Dereference vulnerability in the Captive Portal Content Delivery (CPCD) services daemon (cpcd) of Juniper Networks Junos OS on MX Series with MS-PIC, MS-SPC3, MS-MIC or MS-MPC allows an attacker to send malformed HTTP packets to the device thereby causing a Denial of Service (DoS), crashing the Multiservices PIC Management Daemon (mspmmand) process thereby denying users the ability to login, while concurrently impacting other mspmmand services and traffic through the device. Continued receipt and processing of these malformed packets will create a sustained Denial of Service (DoS) condition. While the Services PIC is restarting, all PIC services will be bypassed until the Services PIC completes its boot process. An attacker sending these malformed HTTP packets to the device who is not part of the Captive Portal experience is not able to exploit this	https://kb.juniper.net/JS_A11144	H-JUN-MX24-040521/523

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>issue. This issue is not applicable to MX RE-based CPCD platforms. This issue affects: Juniper Networks Junos OS on MX Series 17.3 version 17.3R1 and later versions prior to 17.4 versions 17.4R2-S9, 17.4R3-S2; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S3; 18.3 versions prior to 18.3R3-S1; 18.4 versions prior to 18.4R3; 19.1 versions prior to 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R2; 19.3 versions prior to 19.3R3. This issue does not affect: Juniper Networks Junos OS versions prior to 17.3R1.</p> <p>CVE ID : CVE-2021-0251</p>		
Improper Check for Unusual or Exceptional Conditions	22-04-2021	5	<p>An improper check for unusual or exceptional conditions vulnerability in Juniper Networks MX Series platforms with Trio-based MPC (Modular Port Concentrator) deployed in (Ethernet VPN) EVPN- (Virtual Extensible LAN) VXLAN configuration, may allow an attacker sending specific Layer 2 traffic to cause Distributed Denial of Service (DDoS) protection to trigger unexpectedly, resulting in traffic impact. Continued receipt and processing of this specific Layer 2 frames will sustain the Denial of Service (DoS) condition. An indication of</p>	https://kb.juniper.net/JS_A11123	H-JUN-MX24-040521/524

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>compromise is to check DDOS LACP violations: user@device> show ddos-protection protocols statistics brief match lacp</p> <p>This issue only affects the MX Series platforms with Trio-based MPC. No other products or platforms are affected. This issue affects: Juniper Networks Junos OS on MX Series: 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S1, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2;</p> <p>CVE ID : CVE-2021-0228</p>		
Uncontrolled Resource Consumption	22-04-2021	5	<p>On Juniper Networks Junos OS platforms with link aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes</p>	https://kb.juniper.net/JS_A11125	H-JUN-MX24-040521/525

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel: rt_pfe_veto: Memory over consumed. Op 1 err 12, rtsm_id 0:-1, msg type 72 /kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd</p> <p>An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<<</p> <p>user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<< This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000-72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3.</p> <p>CVE ID : CVE-2021-0230</p>		
Improper Handling of Exceptional Conditions	22-04-2021	5	<p>A vulnerability in the processing of traffic matching a firewall filter containing a syslog action in Juniper Networks Junos OS on MX Series with MPC10/MPC11 cards installed, PTX10003 and PTX10008 Series devices, will cause the line card to crash and restart, creating a Denial of Service (DoS). Continued receipt and processing of packets matching the firewall filter</p>	<p>https://kb.juniper.net/JS_A11155, https://kb.juniper.net/TS_B17931</p>	H-JUN-MX24-040521/526

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>can create a sustained Denial of Service (DoS) condition. When traffic hits the firewall filter, configured on lo0 or any physical interface on the line card, containing a term with a syslog action (e.g. 'term <name> then syslog'), the affected line card will crash and restart, impacting traffic processing through the ports of the line card. This issue only affects MX Series routers with MPC10 or MPC11 line cards, and PTX10003 or PTX10008 Series packet transport routers. No other platforms or models of line cards are affected by this issue. Note: This issue has also been identified and described in technical service bulletin TSB17931 (login required). This issue affects: Juniper Networks Junos OS on MX Series: 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2. Juniper Networks Junos OS Evolved on PTX10003, PTX10008: All versions prior to 20.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1.</p>		

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-0264		
mx40					
NULL Pointer Dereference	22-04-2021	5	<p>A NULL Pointer Dereference vulnerability in the Captive Portal Content Delivery (CPCD) services daemon (cpcd) of Juniper Networks Junos OS on MX Series with MS-PIC, MS-SPC3, MS-MIC or MS-MPC allows an attacker to send malformed HTTP packets to the device thereby causing a Denial of Service (DoS), crashing the Multiservices PIC Management Daemon (mospmand) process thereby denying users the ability to login, while concurrently impacting other mospmand services and traffic through the device. Continued receipt and processing of these malformed packets will create a sustained Denial of Service (DoS) condition. While the Services PIC is restarting, all PIC services will be bypassed until the Services PIC completes its boot process. An attacker sending these malformed HTTP packets to the device who is not part of the Captive Portal experience is not able to exploit this issue. This issue is not applicable to MX RE-based CPCD platforms. This issue affects: Juniper Networks Junos OS on MX Series 17.3 version 17.3R1 and later</p>	https://kb.juniper.net/JS_A11144	H-JUN-MX40-040521/527

CVSS Scoring Scale	0-1	1-2	2-3	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 17.4 versions 17.4R2-S9, 17.4R3-S2; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S3; 18.3 versions prior to 18.3R3-S1; 18.4 versions prior to 18.4R3; 19.1 versions prior to 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R2; 19.3 versions prior to 19.3R3. This issue does not affect: Juniper Networks Junos OS versions prior to 17.3R1. CVE ID : CVE-2021-0251		
Uncontrolled Resource Consumption	22-04-2021	2.1	When a MX Series is configured as a Broadband Network Gateway (BNG) based on Layer 2 Tunneling Protocol (L2TP), executing certain CLI command may cause the system to run out of disk space, excessive disk usage may cause other complications. An administrator can use the following CLI command to monitor the available disk space: user@device> show system storage Filesystem Size Used Avail Capacity Mounted on /dev/gpt/junos 19G 18G 147M 99% /.mount <<<<< running out of space tmpfs 21G 16K 21G 0% /.mount/tmp tmpfs 5.3G 1.7M 5.3G 0% /.mount/mfs This issue affects Juniper Networks Junos OS on MX Series: 17.3R1 and later versions prior to 17.4R3-S5,	https://kb.juniper.net/JS_A11133	H-JUN-MX40-040521/528

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>18.1 versions prior to 18.1R3-S13, 18.2 versions prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S7; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2; 20.4 versions prior to 20.4R1-S1, 20.4R2; This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1.</p> <p>CVE ID : CVE-2021-0238</p>		
Improper Check for Unusual or Exceptional Conditions	22-04-2021	5	<p>An improper check for unusual or exceptional conditions vulnerability in Juniper Networks MX Series platforms with Trio-based MPC (Modular Port Concentrator) deployed in (Ethernet VPN) EVPN- (Virtual Extensible LAN) VXLAN configuration, may allow an attacker sending specific Layer 2 traffic to cause Distributed Denial of Service (DDoS) protection to trigger unexpectedly, resulting in traffic impact. Continued receipt and processing of this specific Layer 2 frames will sustain the Denial of Service (DoS) condition. An indication of compromise is to check</p>	https://kb.juniper.net/JS_A11123	H-JUN-MX40-040521/529

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>DDOS LACP violations: user@device> show ddos-protection protocols statistics brief match lacp This issue only affects the MX Series platforms with Trio-based MPC. No other products or platforms are affected. This issue affects: Juniper Networks Junos OS on MX Series: 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S1, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2;</p> <p>CVE ID : CVE-2021-0228</p>		
Uncontrolled Resource Consumption	22-04-2021	5	<p>On Juniper Networks Junos OS platforms with link aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak.</p>	https://kb.juniper.net/JS_A11125	H-JUN-MX40-040521/530

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>If all the available memory is consumed, the traffic will be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel: rt_pfe_veto: Memory over consumed. Op 1 err 12, rtsm_id 0:-1, msg type 72</p> <p>/kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd</p> <p>An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device</p> <pre>> show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<<</pre> <p>user@device > show system virtual-memory no-forwarding match ifstat</p> <pre>Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<<</pre> <p>This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000-72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper Networks EX9200 Series.</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3.</p> <p>CVE ID : CVE-2021-0230</p>		
Improper Handling of Exceptional Conditions	22-04-2021	5	<p>A vulnerability in the processing of traffic matching a firewall filter containing a syslog action in Juniper Networks Junos OS on MX Series with MPC10/MPC11 cards installed, PTX10003 and PTX10008 Series devices, will cause the line card to crash and restart, creating a Denial of Service (DoS). Continued receipt and processing of packets matching the firewall filter can create a sustained</p>	<p>https://kb.juniper.net/JS_A11155, https://kb.juniper.net/TS_B17931</p>	H-JUN-MX40-040521/531

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Denial of Service (DoS) condition. When traffic hits the firewall filter, configured on lo0 or any physical interface on the line card, containing a term with a syslog action (e.g. 'term <name> then syslog'), the affected line card will crash and restart, impacting traffic processing through the ports of the line card. This issue only affects MX Series routers with MPC10 or MPC11 line cards, and PTX10003 or PTX10008 Series packet transport routers. No other platforms or models of line cards are affected by this issue. Note: This issue has also been identified and described in technical service bulletin TSB17931 (login required). This issue affects: Juniper Networks Junos OS on MX Series: 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2. Juniper Networks Junos OS Evolved on PTX10003, PTX10008: All versions prior to 20.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1.</p> <p>CVE ID : CVE-2021-0264</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
mx480											
NULL Pointer Dereference	22-04-2021	5	A NULL Pointer Dereference vulnerability in the Captive Portal Content Delivery (CPCD) services daemon (cpcd) of Juniper Networks Junos OS on MX Series with MS-PIC, MS-SPC3, MS-MIC or MS-MPC allows an attacker to send malformed HTTP packets to the device thereby causing a Denial of Service (DoS), crashing the Multiservices PIC Management Daemon (mospmand) process thereby denying users the ability to login, while concurrently impacting other mospmand services and traffic through the device. Continued receipt and processing of these malformed packets will create a sustained Denial of Service (DoS) condition. While the Services PIC is restarting, all PIC services will be bypassed until the Services PIC completes its boot process. An attacker sending these malformed HTTP packets to the device who is not part of the Captive Portal experience is not able to exploit this issue. This issue is not applicable to MX RE-based CPCD platforms. This issue affects: Juniper Networks Junos OS on MX Series 17.3 version 17.3R1 and later versions prior to 17.4 versions 17.4R2-S9, 17.4R3-	https://kb.juniper.net/JS_A11144	H-JUN-MX48-040521/532						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S2; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S3; 18.3 versions prior to 18.3R3-S1; 18.4 versions prior to 18.4R3; 19.1 versions prior to 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R2; 19.3 versions prior to 19.3R3. This issue does not affect: Juniper Networks Junos OS versions prior to 17.3R1. CVE ID : CVE-2021-0251		
Uncontrolled Resource Consumption	22-04-2021	2.1	When a MX Series is configured as a Broadband Network Gateway (BNG) based on Layer 2 Tunneling Protocol (L2TP), executing certain CLI command may cause the system to run out of disk space, excessive disk usage may cause other complications. An administrator can use the following CLI command to monitor the available disk space: user@device> show system storage Filesystem Size Used Avail Capacity Mounted on /dev/gpt/junos 19G 18G 147M 99% /.mount <<<<< running out of space tmpfs 21G 16K 21G 0% /.mount/tmp tmpfs 5.3G 1.7M 5.3G 0% /.mount/mfs This issue affects Juniper Networks Junos OS on MX Series: 17.3R1 and later versions prior to 17.4R3-S5, 18.1 versions prior to 18.1R3-S13, 18.2 versions	https://kb.juniper.net/JS_A11133	H-JUN-MX48-040521/533

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S7; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2; 20.4 versions prior to 20.4R1-S1, 20.4R2; This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1.</p> <p>CVE ID : CVE-2021-0238</p>		
Improper Check for Unusual or Exceptional Conditions	22-04-2021	5	<p>An improper check for unusual or exceptional conditions vulnerability in Juniper Networks MX Series platforms with Trio-based MPC (Modular Port Concentrator) deployed in (Ethernet VPN) EVPN- (Virtual Extensible LAN) VXLAN configuration, may allow an attacker sending specific Layer 2 traffic to cause Distributed Denial of Service (DDoS) protection to trigger unexpectedly, resulting in traffic impact. Continued receipt and processing of this specific Layer 2 frames will sustain the Denial of Service (DoS) condition. An indication of compromise is to check DDOS LACP violations: user@device> show ddos-</p>	https://kb.juniper.net/JS_A11123	H-JUN-MX48-040521/534

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>protection protocols statistics brief match lacp This issue only affects the MX Series platforms with Trio-based MPC. No other products or platforms are affected. This issue affects: Juniper Networks Junos OS on MX Series: 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S1, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2;</p> <p>CVE ID : CVE-2021-0228</p>		
Uncontrolled Resource Consumption	22-04-2021	5	<p>On Juniper Networks Junos OS platforms with link aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak. If all the available memory is consumed, the traffic will</p>	https://kb.juniper.net/JS_A11125	H-JUN-MX48-040521/535

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel: rt_pfe_veto: Memory over consumed. Op 1 err 12, rtsm_id 0:-1, msg type 72 /kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd</p> <p>An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<<</p> <p>user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<< This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000-72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Networks NFX Series. This issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3.</p> <p>CVE ID : CVE-2021-0230</p>		
Improper Handling of Exceptional Conditions	22-04-2021	5	<p>A vulnerability in the processing of traffic matching a firewall filter containing a syslog action in Juniper Networks Junos OS on MX Series with MPC10/MPC11 cards installed, PTX10003 and PTX10008 Series devices, will cause the line card to crash and restart, creating a Denial of Service (DoS). Continued receipt and processing of packets matching the firewall filter can create a sustained Denial of Service (DoS) condition. When traffic hits</p>	<p>https://kb.juniper.net/JS_A11155, https://kb.juniper.net/TS_B17931</p>	H-JUN-MX48-040521/536

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			<p>the firewall filter, configured on lo0 or any physical interface on the line card, containing a term with a syslog action (e.g. 'term <name> then syslog'), the affected line card will crash and restart, impacting traffic processing through the ports of the line card. This issue only affects MX Series routers with MPC10 or MPC11 line cards, and PTX10003 or PTX10008 Series packet transport routers. No other platforms or models of line cards are affected by this issue. Note: This issue has also been identified and described in technical service bulletin TSB17931 (login required). This issue affects: Juniper Networks Junos OS on MX Series: 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2. Juniper Networks Junos OS Evolved on PTX10003, PTX10008: All versions prior to 20.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1.</p> <p>CVE ID : CVE-2021-0264</p>							
mx5										
NULL Pointer	22-04-2021	5	A NULL Pointer Dereference	https://kb.ju	H-JUN-MX5-					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			<p>vulnerability in the Captive Portal Content Delivery (CPCD) services daemon (cpcd) of Juniper Networks Junos OS on MX Series with MS-PIC, MS-SPC3, MS-MIC or MS-MPC allows an attacker to send malformed HTTP packets to the device thereby causing a Denial of Service (DoS), crashing the Multiservices PIC Management Daemon (mispmand) process thereby denying users the ability to login, while concurrently impacting other mispmand services and traffic through the device. Continued receipt and processing of these malformed packets will create a sustained Denial of Service (DoS) condition. While the Services PIC is restarting, all PIC services will be bypassed until the Services PIC completes its boot process. An attacker sending these malformed HTTP packets to the device who is not part of the Captive Portal experience is not able to exploit this issue. This issue is not applicable to MX RE-based CPCD platforms. This issue affects: Juniper Networks Junos OS on MX Series 17.3 version 17.3R1 and later versions prior to 17.4 versions 17.4R2-S9, 17.4R3-S2; 18.1 versions prior to 18.1R3-S9; 18.2 versions</p>	niper.net/JS A11144	040521/537

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>prior to 18.2R3-S3; 18.3 versions prior to 18.3R3-S1; 18.4 versions prior to 18.4R3; 19.1 versions prior to 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R2; 19.3 versions prior to 19.3R3. This issue does not affect: Juniper Networks Junos OS versions prior to 17.3R1.</p> <p>CVE ID : CVE-2021-0251</p>		
Uncontrolled Resource Consumption	22-04-2021	2.1	<p>When a MX Series is configured as a Broadband Network Gateway (BNG) based on Layer 2 Tunneling Protocol (L2TP), executing certain CLI command may cause the system to run out of disk space, excessive disk usage may cause other complications. An administrator can use the following CLI command to monitor the available disk space: user@device> show system storage Filesystem Size Used Avail Capacity Mounted on</p> <pre> /dev/gpt/junos 19G 18G 147M 99% /.mount <<<<< running out of space tmpfs 21G 16K 21G 0% /.mount/tmp tmpfs 5.3G 1.7M 5.3G 0% /.mount/mfs </pre> <p>This issue affects Juniper Networks Junos OS on MX Series: 17.3R1 and later versions prior to 17.4R3-S5, 18.1 versions prior to 18.1R3-S13, 18.2 versions prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4;</p>	https://kb.juniper.net/JS_A11133	H-JUN-MX5-040521/538

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.4 versions prior to 18.4R3-S7; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2; 20.4 versions prior to 20.4R1-S1, 20.4R2; This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1. CVE ID : CVE-2021-0238		
Improper Check for Unusual or Exceptional Conditions	22-04-2021	5	An improper check for unusual or exceptional conditions vulnerability in Juniper Networks MX Series platforms with Trio-based MPC (Modular Port Concentrator) deployed in (Ethernet VPN) EVPN- (Virtual Extensible LAN) VXLAN configuration, may allow an attacker sending specific Layer 2 traffic to cause Distributed Denial of Service (DDoS) protection to trigger unexpectedly, resulting in traffic impact. Continued receipt and processing of this specific Layer 2 frames will sustain the Denial of Service (DoS) condition. An indication of compromise is to check DDOS LACP violations: user@device> show ddos-protection protocols statistics brief match lacp	https://kb.juniper.net/JS_A11123	H-JUN-MX5-040521/539

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>This issue only affects the MX Series platforms with Trio-based MPC. No other products or platforms are affected. This issue affects: Juniper Networks Junos OS on MX Series: 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S1, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2;</p> <p>CVE ID : CVE-2021-0228</p>		
Uncontrolled Resource Consumption	22-04-2021	5	<p>On Juniper Networks Junos OS platforms with link aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot might be required. The</p>	https://kb.juniper.net/JS_A11125	H-JUN-MX5-040521/540

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>following log can be seen if this issue happens. /kernel: rt_pfe_veto: Memory over consumed. Op 1 err 12, rtsm_id 0:-1, msg type 72</p> <p>/kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd</p> <p>An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device</p> <pre>> show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<<</pre> <p>user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<<</p> <p>This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000-72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This issue affects Juniper</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Networks Junos OS: 17.1 versions 17.1R3 and above prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3.</p> <p>CVE ID : CVE-2021-0230</p>		
Improper Handling of Exceptional Conditions	22-04-2021	5	<p>A vulnerability in the processing of traffic matching a firewall filter containing a syslog action in Juniper Networks Junos OS on MX Series with MPC10/MPC11 cards installed, PTX10003 and PTX10008 Series devices, will cause the line card to crash and restart, creating a Denial of Service (DoS). Continued receipt and processing of packets matching the firewall filter can create a sustained Denial of Service (DoS) condition. When traffic hits the firewall filter, configured on lo0 or any</p>	<p>https://kb.juniper.net/JS_A11155, https://kb.juniper.net/TS_B17931</p>	H-JUN-MX5-040521/541

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			physical interface on the line card, containing a term with a syslog action (e.g. 'term <name> then syslog'), the affected line card will crash and restart, impacting traffic processing through the ports of the line card. This issue only affects MX Series routers with MPC10 or MPC11 line cards, and PTX10003 or PTX10008 Series packet transport routers. No other platforms or models of line cards are affected by this issue. Note: This issue has also been identified and described in technical service bulletin TSB17931 (login required). This issue affects: Juniper Networks Junos OS on MX Series: 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2. Juniper Networks Junos OS Evolved on PTX10003, PTX10008: All versions prior to 20.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1. CVE ID : CVE-2021-0264							
mx80										
NULL Pointer Dereference	22-04-2021	5	A NULL Pointer Dereference vulnerability in the Captive Portal Content Delivery	https://kb.juniper.net/JS_A11144	H-JUN-MX80-040521/542					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>(CPCD) services daemon (cpcd) of Juniper Networks Junos OS on MX Series with MS-PIC, MS-SPC3, MS-MIC or MS-MPC allows an attacker to send malformed HTTP packets to the device thereby causing a Denial of Service (DoS), crashing the Multiservices PIC Management Daemon (mspmmand) process thereby denying users the ability to login, while concurrently impacting other mspmand services and traffic through the device. Continued receipt and processing of these malformed packets will create a sustained Denial of Service (DoS) condition. While the Services PIC is restarting, all PIC services will be bypassed until the Services PIC completes its boot process. An attacker sending these malformed HTTP packets to the device who is not part of the Captive Portal experience is not able to exploit this issue. This issue is not applicable to MX RE-based CPCD platforms. This issue affects: Juniper Networks Junos OS on MX Series 17.3 version 17.3R1 and later versions prior to 17.4 versions 17.4R2-S9, 17.4R3-S2; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S3; 18.3 versions prior to 18.3R3-S1;</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.4 versions prior to 18.4R3; 19.1 versions prior to 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R2; 19.3 versions prior to 19.3R3. This issue does not affect: Juniper Networks Junos OS versions prior to 17.3R1. CVE ID : CVE-2021-0251		
Uncontrolled Resource Consumption	22-04-2021	2.1	When a MX Series is configured as a Broadband Network Gateway (BNG) based on Layer 2 Tunneling Protocol (L2TP), executing certain CLI command may cause the system to run out of disk space, excessive disk usage may cause other complications. An administrator can use the following CLI command to monitor the available disk space: user@device> show system storage Filesystem Size Used Avail Capacity Mounted on /dev/gpt/junos 19G 18G 147M 99% /.mount <<<<< running out of space tmpfs 21G 16K 21G 0% /.mount/tmp tmpfs 5.3G 1.7M 5.3G 0% /.mount/mfs This issue affects Juniper Networks Junos OS on MX Series: 17.3R1 and later versions prior to 17.4R3-S5, 18.1 versions prior to 18.1R3-S13, 18.2 versions prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S7; 19.1 versions	https://kb.juniper.net/JS_A11133	H-JUN-MX80-040521/543

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2; 20.4 versions prior to 20.4R1-S1, 20.4R2; This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1.</p> <p>CVE ID : CVE-2021-0238</p>		
Improper Check for Unusual or Exceptional Conditions	22-04-2021	5	<p>An improper check for unusual or exceptional conditions vulnerability in Juniper Networks MX Series platforms with Trio-based MPC (Modular Port Concentrator) deployed in (Ethernet VPN) EVPN- (Virtual Extensible LAN) VXLAN configuration, may allow an attacker sending specific Layer 2 traffic to cause Distributed Denial of Service (DDoS) protection to trigger unexpectedly, resulting in traffic impact. Continued receipt and processing of this specific Layer 2 frames will sustain the Denial of Service (DoS) condition. An indication of compromise is to check DDOS LACP violations: user@device> show ddos-protection protocols statistics brief match lacp This issue only affects the MX Series platforms with</p>	https://kb.juniper.net/JS_A11123	H-JUN-MX80-040521/544

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Trio-based MPC. No other products or platforms are affected. This issue affects: Juniper Networks Junos OS on MX Series: 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S1, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2;</p> <p>CVE ID : CVE-2021-0228</p>		
Uncontrolled Resource Consumption	22-04-2021	5	<p>On Juniper Networks Junos OS platforms with link aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel:</p>	https://kb.juniper.net/JS_A11125	H-JUN-MX80-040521/545

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>rt_pfe_veto: Memory over consumed. Op 1 err 12, rtsm_id 0:-1, msg type 72 /kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd</p> <p>An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<<</p> <p>user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<< This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000-72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3.</p> <p>CVE ID : CVE-2021-0230</p>		
Improper Handling of Exceptional Conditions	22-04-2021	5	<p>A vulnerability in the processing of traffic matching a firewall filter containing a syslog action in Juniper Networks Junos OS on MX Series with MPC10/MPC11 cards installed, PTX10003 and PTX10008 Series devices, will cause the line card to crash and restart, creating a Denial of Service (DoS). Continued receipt and processing of packets matching the firewall filter can create a sustained Denial of Service (DoS) condition. When traffic hits the firewall filter, configured on lo0 or any physical interface on the line card, containing a term</p>	<p>https://kb.juniper.net/JS_A11155, https://kb.juniper.net/TS_B17931</p>	H-JUN-MX80-040521/546

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>with a syslog action (e.g. 'term <name> then syslog'), the affected line card will crash and restart, impacting traffic processing through the ports of the line card. This issue only affects MX Series routers with MPC10 or MPC11 line cards, and PTX10003 or PTX10008 Series packet transport routers. No other platforms or models of line cards are affected by this issue. Note: This issue has also been identified and described in technical service bulletin TSB17931 (login required). This issue affects: Juniper Networks Junos OS on MX Series: 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2. Juniper Networks Junos OS Evolved on PTX10003, PTX10008: All versions prior to 20.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1.</p> <p>CVE ID : CVE-2021-0264</p>		
mx960					
NULL Pointer Dereference	22-04-2021	5	A NULL Pointer Dereference vulnerability in the Captive Portal Content Delivery (CPCD) services daemon (cpcd) of Juniper Networks	https://kb.juniper.net/JS_A11144	H-JUN-MX96-040521/547

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Junos OS on MX Series with MS-PIC, MS-SPC3, MS-MIC or MS-MPC allows an attacker to send malformed HTTP packets to the device thereby causing a Denial of Service (DoS), crashing the Multiservices PIC Management Daemon (mospmand) process thereby denying users the ability to login, while concurrently impacting other mospmand services and traffic through the device. Continued receipt and processing of these malformed packets will create a sustained Denial of Service (DoS) condition. While the Services PIC is restarting, all PIC services will be bypassed until the Services PIC completes its boot process. An attacker sending these malformed HTTP packets to the device who is not part of the Captive Portal experience is not able to exploit this issue. This issue is not applicable to MX RE-based CPCD platforms. This issue affects: Juniper Networks Junos OS on MX Series 17.3 version 17.3R1 and later versions prior to 17.4 versions 17.4R2-S9, 17.4R3-S2; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S3; 18.3 versions prior to 18.3R3-S1; 18.4 versions prior to 18.4R3; 19.1 versions prior</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R2; 19.3 versions prior to 19.3R3. This issue does not affect: Juniper Networks Junos OS versions prior to 17.3R1. CVE ID : CVE-2021-0251		
Uncontrolled Resource Consumption	22-04-2021	2.1	When a MX Series is configured as a Broadband Network Gateway (BNG) based on Layer 2 Tunneling Protocol (L2TP), executing certain CLI command may cause the system to run out of disk space, excessive disk usage may cause other complications. An administrator can use the following CLI command to monitor the available disk space: user@device> show system storage Filesystem Size Used Avail Capacity Mounted on /dev/gpt/junos 19G 18G 147M 99% /.mount <<<<< running out of space tmpfs 21G 16K 21G 0% /.mount/tmp tmpfs 5.3G 1.7M 5.3G 0% /.mount/mfs This issue affects Juniper Networks Junos OS on MX Series: 17.3R1 and later versions prior to 17.4R3-S5, 18.1 versions prior to 18.1R3-S13, 18.2 versions prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S7; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6,	https://kb.juniper.net/JS_A11133	H-JUN-MX96-040521/548

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2; 20.4 versions prior to 20.4R1-S1, 20.4R2; This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1. CVE ID : CVE-2021-0238		
Improper Check for Unusual or Exceptional Conditions	22-04-2021	5	An improper check for unusual or exceptional conditions vulnerability in Juniper Networks MX Series platforms with Trio-based MPC (Modular Port Concentrator) deployed in (Ethernet VPN) EVPN- (Virtual Extensible LAN) VXLAN configuration, may allow an attacker sending specific Layer 2 traffic to cause Distributed Denial of Service (DDoS) protection to trigger unexpectedly, resulting in traffic impact. Continued receipt and processing of this specific Layer 2 frames will sustain the Denial of Service (DoS) condition. An indication of compromise is to check DDOS LACP violations: user@device> show ddos-protection protocols statistics brief match lacp This issue only affects the MX Series platforms with Trio-based MPC. No other products or platforms are	https://kb.juniper.net/JS_A11123	H-JUN-MX96-040521/549

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>affected. This issue affects: Juniper Networks Junos OS on MX Series: 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S1, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2;</p> <p>CVE ID : CVE-2021-0228</p>		
Uncontrolled Resource Consumption	22-04-2021	5	<p>On Juniper Networks Junos OS platforms with link aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel: rt_pfe_veto: Memory over consumed. Op 1 err 12,</p>	https://kb.juniper.net/JS_A11125	H-JUN-MX96-040521/550

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>rtsm_id 0:-1, msg type 72 /kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device > show system virtual- memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<< user@device > show system virtual-memory no- forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<< This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000- 72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5;</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3.</p> <p>CVE ID : CVE-2021-0230</p>		
Improper Handling of Exceptional Conditions	22-04-2021	5	<p>A vulnerability in the processing of traffic matching a firewall filter containing a syslog action in Juniper Networks Junos OS on MX Series with MPC10/MPC11 cards installed, PTX10003 and PTX10008 Series devices, will cause the line card to crash and restart, creating a Denial of Service (DoS). Continued receipt and processing of packets matching the firewall filter can create a sustained Denial of Service (DoS) condition. When traffic hits the firewall filter, configured on lo0 or any physical interface on the line card, containing a term with a syslog action (e.g. 'term <name> then syslog'),</p>	<p>https://kb.juniper.net/JS_A11155, https://kb.juniper.net/TS_B17931</p>	H-JUN-MX96-040521/551

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>the affected line card will crash and restart, impacting traffic processing through the ports of the line card. This issue only affects MX Series routers with MPC10 or MPC11 line cards, and PTX10003 or PTX10008 Series packet transport routers. No other platforms or models of line cards are affected by this issue. Note: This issue has also been identified and described in technical service bulletin TSB17931 (login required). This issue affects: Juniper Networks Junos OS on MX Series: 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2. Juniper Networks Junos OS Evolved on PTX10003, PTX10008: All versions prior to 20.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1.</p> <p>CVE ID : CVE-2021-0264</p>		
nfx150					
Improper Neutralization of Special Elements used in a Command ('Command	22-04-2021	4.6	<p>NFX Series devices using Juniper Networks Junos OS are susceptible to a local code execution vulnerability thereby allowing an attacker to elevate their privileges via</p>	https://kb.juniper.net/JS_A11145	H-JUN-NFX1-040521/552

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			<p>the Junos Device Management Daemon (JDMD) process. This issue affects Juniper Networks Junos OS on NFX Series: 18.1 version 18.1R1 and later versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R1-S3, 19.1R2; 19.2 versions prior to 19.2R1-S5, 19.2R2. This issue does not affect: Juniper Networks Junos OS versions prior to 18.1R1. This issue does not affect the JDMD as used by Junos Node Slicing such as External Servers use in conjunction with Junos Node Slicing and In-Chassis Junos Node Slicing on MX480, MX960, MX2008, MX2010, MX2020.</p> <p>CVE ID : CVE-2021-0252</p>		
Uncontrolled Resource Consumption	22-04-2021	5	<p>On Juniper Networks Junos OS platforms with link aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel:</p>	https://kb.juniper.net/JS_A11125	H-JUN-NFX1-040521/553

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>rt_pfe_veto: Memory over consumed. Op 1 err 12, rtsm_id 0:-1, msg type 72 /kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd</p> <p>An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<<</p> <p>user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<< This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000-72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3.</p> <p>CVE ID : CVE-2021-0230</p>		
Use of Hard-coded Credentials	22-04-2021	7.5	<p>This issue is not applicable to NFX NextGen Software. On NFX Series devices the use of Hard-coded Credentials in Juniper Networks Junos OS allows an attacker to take over any instance of an NFX deployment. This issue is only exploitable through administrative interfaces. This issue affects: Juniper Networks Junos OS versions prior to 19.1R1 on NFX Series. No other platforms besides NFX Series devices are affected.</p> <p>CVE ID : CVE-2021-0248</p>	https://kb.juniper.net/JS_A11141	H-JUN-NFX1-040521/554
Improper Neutralization of Special Elements	22-04-2021	4.6	<p>NFX Series devices using Juniper Networks Junos OS are susceptible to a local command execution</p>	https://kb.juniper.net/JS_A11146	H-JUN-NFX1-040521/555

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			<p>vulnerability thereby allowing an attacker to elevate their privileges via the Junos Device Management Daemon (JDMD) process. This issue affects Juniper Networks Junos OS on NFX Series 17.2 version 17.2R1 and later versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S5, 18.4R3-S5; 19.1 versions prior to 19.1R1-S3; 19.2 version 19.1R2 and later versions prior to 19.2R3; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2-S2. 19.4 versions 19.4R3 and above. This issue does not affect Juniper Networks Junos OS versions prior to 17.2R1. This issue does not affect the JDMD as used by Junos Node Slicing such as External Servers use in conjunction with Junos Node Slicing and In-Chassis Junos Node Slicing on MX480, MX960, MX2008, MX2010, MX2020.</p> <p>CVE ID : CVE-2021-0253</p>		
nfx250					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-04-2021	4.6	<p>NFX Series devices using Juniper Networks Junos OS are susceptible to a local code execution vulnerability thereby allowing an attacker to elevate their privileges via the Junos Device Management Daemon (JDMD) process. This issue</p>	https://kb.juniper.net/JS_A11145	H-JUN-NFX2-040521/556

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>affects Juniper Networks Junos OS on NFX Series: 18.1 version 18.1R1 and later versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R1-S3, 19.1R2; 19.2 versions prior to 19.2R1-S5, 19.2R2. This issue does not affect: Juniper Networks Junos OS versions prior to 18.1R1. This issue does not affect the JDMD as used by Junos Node Slicing such as External Servers use in conjunction with Junos Node Slicing and In-Chassis Junos Node Slicing on MX480, MX960, MX2008, MX2010, MX2020.</p> <p>CVE ID : CVE-2021-0252</p>		
Uncontrolled Resource Consumption	22-04-2021	5	<p>On Juniper Networks Junos OS platforms with link aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel: rt_pfe_veto: Memory over consumed. Op 1 err 12, rtsm_id 0:-1, msg type 72</p>	https://kb.juniper.net/JS_A11125	H-JUN-NFX2-040521/557

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			/kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device > show system virtual- memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<< user@device > show system virtual-memory no- forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<< This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000- 72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3. CVE ID : CVE-2021-0230								
Use of Hard-coded Credentials	22-04-2021	7.5	This issue is not applicable to NFX NextGen Software. On NFX Series devices the use of Hard-coded Credentials in Juniper Networks Junos OS allows an attacker to take over any instance of an NFX deployment. This issue is only exploitable through administrative interfaces. This issue affects: Juniper Networks Junos OS versions prior to 19.1R1 on NFX Series. No other platforms besides NFX Series devices are affected. CVE ID : CVE-2021-0248	https://kb.juniper.net/JS_A11141	H-JUN-NFX2-040521/558						
Improper Neutralization of Special Elements used in a Command ('Command	22-04-2021	4.6	NFX Series devices using Juniper Networks Junos OS are susceptible to a local command execution vulnerability thereby allowing an attacker to elevate their privileges via	https://kb.juniper.net/JS_A11146	H-JUN-NFX2-040521/559						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			<p>the Junos Device Management Daemon (JDMD) process. This issue affects Juniper Networks Junos OS on NFX Series 17.2 version 17.2R1 and later versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S5, 18.4R3-S5; 19.1 versions prior to 19.1R1-S3; 19.2 version 19.1R2 and later versions prior to 19.2R3; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2-S2. 19.4 versions 19.4R3 and above. This issue does not affect Juniper Networks Junos OS versions prior to 17.2R1. This issue does not affect the JDMD as used by Junos Node Slicing such as External Servers use in conjunction with Junos Node Slicing and In-Chassis Junos Node Slicing on MX480, MX960, MX2008, MX2010, MX2020.</p> <p>CVE ID : CVE-2021-0253</p>		
nfx350					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-04-2021	4.6	<p>NFX Series devices using Juniper Networks Junos OS are susceptible to a local code execution vulnerability thereby allowing an attacker to elevate their privileges via the Junos Device Management Daemon (JDMD) process. This issue affects Juniper Networks Junos OS on NFX Series: 18.1 version 18.1R1 and</p>	https://kb.juniper.net/JS_A11145	H-JUN-NFX3-040521/560

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>later versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R1-S3, 19.1R2; 19.2 versions prior to 19.2R1-S5, 19.2R2. This issue does not affect: Juniper Networks Junos OS versions prior to 18.1R1. This issue does not affect the JDMD as used by Junos Node Slicing such as External Servers use in conjunction with Junos Node Slicing and In-Chassis Junos Node Slicing on MX480, MX960, MX2008, MX2010, MX2020.</p> <p>CVE ID : CVE-2021-0252</p>		
Uncontrolled Resource Consumption	22-04-2021	5	<p>On Juniper Networks Junos OS platforms with link aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel: rt_pfe_veto: Memory over consumed. Op 1 err 12, rtsm_id 0:-1, msg type 72 /kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd</p>	https://kb.juniper.net/JS_A11125	H-JUN-NFX3-040521/561

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<<</p> <p>user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<< This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000-72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to</p>		

CVSS Scoring Scale	0-1	1-2	2-3	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-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3. CVE ID : CVE-2021-0230		
Use of Hard-coded Credentials	22-04-2021	7.5	This issue is not applicable to NFX NextGen Software. On NFX Series devices the use of Hard-coded Credentials in Juniper Networks Junos OS allows an attacker to take over any instance of an NFX deployment. This issue is only exploitable through administrative interfaces. This issue affects: Juniper Networks Junos OS versions prior to 19.1R1 on NFX Series. No other platforms besides NFX Series devices are affected. CVE ID : CVE-2021-0248	https://kb.juniper.net/JS_A11141	H-JUN-NFX3-040521/562
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-04-2021	4.6	NFX Series devices using Juniper Networks Junos OS are susceptible to a local command execution vulnerability thereby allowing an attacker to elevate their privileges via the Junos Device Management Daemon (JDMD) process. This issue	https://kb.juniper.net/JS_A11146	H-JUN-NFX3-040521/563

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>affects Juniper Networks Junos OS on NFX Series 17.2 version 17.2R1 and later versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S5, 18.4R3-S5; 19.1 versions prior to 19.1R1-S3; 19.2 version 19.1R2 and later versions prior to 19.2R3; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2-S2. 19.4 versions 19.4R3 and above. This issue does not affect Juniper Networks Junos OS versions prior to 17.2R1. This issue does not affect the JDMD as used by Junos Node Slicing such as External Servers use in conjunction with Junos Node Slicing and In-Chassis Junos Node Slicing on MX480, MX960, MX2008, MX2010, MX2020.</p> <p>CVE ID : CVE-2021-0253</p>		
ptx1000					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	4.3	<p>On PTX Series and QFX10k Series devices with the "inline-jflow" feature enabled, a use after free weakness in the Packet Forwarding Engine (PFE) microkernel architecture of Juniper Networks Junos OS may allow an attacker to cause a Denial of Service (DoS) condition whereby one or more Flexible PIC Concentrators (FPCs) may restart. As this is a race condition situation this issue become more likely to</p>	<p>https://kb.juniper.net/JS_A11161, https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/inline-flow-monitoring-ptx.html</p>	H-JUN-PTX1-040521/564

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>be hit when network instability occurs, such as but not limited to BGP/IGP reconvergences, and/or further likely to occur when more active "traffic flows" are occurring through the device. When this issue occurs, it will cause one or more FPCs to restart unexpectedly. During FPC restarts core files will be generated. While the core file is generated traffic will be disrupted. Sustained receipt of large traffic flows and reconvergence-like situations may sustain the Denial of Service (DoS) situation. This issue affects: Juniper Networks Junos OS: 18.1 version 18.1R2 and later versions prior to 18.1R3-S10 on PTX Series, QFX10K Series.</p> <p>CVE ID : CVE-2021-0270</p>		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	6.8	<p>A Race Condition (Concurrent Execution using Shared Resource with Improper Synchronization) vulnerability in the firewall process (dfwd) of Juniper Networks Junos OS allows an attacker to bypass the firewall rule sets applied to the input loopback filter on any interfaces of a device. This issue is detectable by reviewing the PFE firewall rules, as well as the firewall counters and seeing if they are incrementing or not. For example: show firewall</p>	https://kb.juniper.net/JS_A11140	H-JUN-PTX1-040521/565

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Filter: __default_bpdu_filter__ Filter: FILTER-INET-01 Counters: Name Bytes Packets output-match-inet 0 0 <<<<< missing firewall packet count This issue affects: Juniper Networks Junos OS 14.1X53 versions prior to 14.1X53-D53 on QFX Series; 14.1 versions 14.1R1 and later versions prior to 15.1 versions prior to 15.1R7-S6 on QFX Series, PTX Series; 15.1X53 versions prior to 15.1X53- D593 on QFX Series; 16.1 versions prior to 16.1R7-S7 on QFX Series, PTX Series; 16.2 versions prior to 16.2R2-S11, 16.2R3 on QFX Series, PTX Series; 17.1 versions prior to 17.1R2- S11, 17.1R3-S2 on QFX Series, PTX Series; 17.2 versions prior to 17.2R1-S9, 17.2R3-S3 on QFX Series, PTX Series; 17.3 versions prior to 17.3R2-S5, 17.3R3- S7 on QFX Series, PTX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3 on QFX Series, PTX Series; 18.1 versions prior to 18.1R3-S9 on QFX Series, PTX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on QFX Series, PTX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1 on QFX Series, PTX Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R2-S7, 18.4R3 on QFX Series, PTX</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on QFX Series, PTX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on QFX Series, PTX Series. CVE ID : CVE-2021-0247		
ptx1000-72q					
Uncontrolled Resource Consumption	22-04-2021	5	On Juniper Networks Junos OS platforms with link aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel: rt_pfe_veto: Memory over consumed. Op 1 err 12, rtsm_id 0:-1, msg type 72 /kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<< user@device > show system	https://kb.juniper.net/JS_A11125	H-JUN-PTX1-040521/566

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>virtual-memory no-forwarding match ifstat</p> <p>Type InUse MemUse</p> <p>HighUse Limit Requests</p> <p>Limit Limit Size(s) ifstat</p> <p>3021629 189749K -</p> <p>22914415 <<<< This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000-72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			17.1R3. CVE ID : CVE-2021-0230		
ptx10001					
Uncontrolled Resource Consumption	22-04-2021	5	<p>On Juniper Networks Junos OS platforms with link aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel: rt_pfe_veto: Memory over consumed. Op 1 err 12, rtsm_id 0:-1, msg type 72 /kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd</p> <p>An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<<</p> <p>user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat</p>	https://kb.juniper.net/JS_A11125	H-JUN-PTX1-040521/567

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			3021629 189749K - 22914415 <<<< This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000-72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3. CVE ID : CVE-2021-0230							
ptx10001-36mr										
Concurrent	22-04-2021	4.3	On PTX Series and QFX10k	https://kb.ju	H-JUN-					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Execution using Shared Resource with Improper Synchronization ('Race Condition')			<p>Series devices with the "inline-jflow" feature enabled, a use after free weakness in the Packet Forwarding Engine (PFE) microkernel architecture of Juniper Networks Junos OS may allow an attacker to cause a Denial of Service (DoS) condition whereby one or more Flexible PIC Concentrators (FPCs) may restart. As this is a race condition situation this issue become more likely to be hit when network instability occurs, such as but not limited to BGP/IGP reconvergences, and/or further likely to occur when more active "traffic flows" are occurring through the device. When this issue occurs, it will cause one or more FPCs to restart unexpectedly. During FPC restarts core files will be generated. While the core file is generated traffic will be disrupted. Sustained receipt of large traffic flows and reconvergence-like situations may sustain the Denial of Service (DoS) situation. This issue affects: Juniper Networks Junos OS: 18.1 version 18.1R2 and later versions prior to 18.1R3-S10 on PTX Series, QFX10K Series.</p> <p>CVE ID : CVE-2021-0270</p>	niper.net/JS A11161, https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/inline-flow-monitoring-ptx.html	PTX1-040521/568
Concurrent Execution	22-04-2021	6.8	A Race Condition (Concurrent Execution	https://kb.juniper.net/JS	H-JUN-PTX1-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
using Shared Resource with Improper Synchronization ('Race Condition')			<p>using Shared Resource with Improper Synchronization) vulnerability in the firewall process (dfwd) of Juniper Networks Junos OS allows an attacker to bypass the firewall rule sets applied to the input loopback filter on any interfaces of a device. This issue is detectable by reviewing the PFE firewall rules, as well as the firewall counters and seeing if they are incrementing or not. For example: show firewall Filter:</p> <pre>__default_bpdu_filter__ Filter: FILTER-INET-01 Counters: Name Bytes Packets output-match-inet 0 0 <<<<<< missing firewall packet count</pre> <p>This issue affects: Juniper Networks Junos OS 14.1X53 versions prior to 14.1X53-D53 on QFX Series; 14.1 versions 14.1R1 and later versions prior to 15.1 versions prior to 15.1R7-S6 on QFX Series, PTX Series; 15.1X53 versions prior to 15.1X53-D593 on QFX Series; 16.1 versions prior to 16.1R7-S7 on QFX Series, PTX Series; 16.2 versions prior to 16.2R2-S11, 16.2R3 on QFX Series, PTX Series; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2 on QFX Series, PTX Series; 17.2 versions prior to 17.2R1-S9, 17.2R3-S3 on QFX Series, PTX Series; 17.3 versions prior to 17.3R2-S5, 17.3R3-</p>	A11140	040521/569

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>S7 on QFX Series, PTX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3 on QFX Series, PTX Series; 18.1 versions prior to 18.1R3-S9 on QFX Series, PTX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on QFX Series, PTX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1 on QFX Series, PTX Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R2-S7, 18.4R3 on QFX Series, PTX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on QFX Series, PTX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on QFX Series, PTX Series.</p> <p>CVE ID : CVE-2021-0247</p>		

ptx10002

Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	4.3	<p>On PTX Series and QFX10k Series devices with the "inline-jflow" feature enabled, a use after free weakness in the Packet Forwarding Engine (PFE) microkernel architecture of Juniper Networks Junos OS may allow an attacker to cause a Denial of Service (DoS) condition whereby one or more Flexible PIC Concentrators (FPCs) may restart. As this is a race condition situation this issue become more likely to be hit when network instability occurs, such as but not limited to BGP/IGP reconvergences, and/or</p>	<p>https://kb.juniper.net/JS_A11161, https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/inline-flow-monitoring-ptx.html</p>	H-JUN-PTX1-040521/570
---	------------	-----	--	--	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			further likely to occur when more active "traffic flows" are occurring through the device. When this issue occurs, it will cause one or more FPCs to restart unexpectedly. During FPC restarts core files will be generated. While the core file is generated traffic will be disrupted. Sustained receipt of large traffic flows and reconvergence-like situations may sustain the Denial of Service (DoS) situation. This issue affects: Juniper Networks Junos OS: 18.1 version 18.1R2 and later versions prior to 18.1R3-S10 on PTX Series, QFX10K Series. CVE ID : CVE-2021-0270		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	6.8	A Race Condition (Concurrent Execution using Shared Resource with Improper Synchronization) vulnerability in the firewall process (dfwd) of Juniper Networks Junos OS allows an attacker to bypass the firewall rule sets applied to the input loopback filter on any interfaces of a device. This issue is detectable by reviewing the PFE firewall rules, as well as the firewall counters and seeing if they are incrementing or not. For example: show firewall Filter: __default_bpdu_filter__ Filter: FILTER-INET-01 Counters: Name Bytes	https://kb.juniper.net/JS_A11140	H-JUN-PTX1-040521/571

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Packets output-match-inet 0 0 <<<<<< missing firewall packet count This issue affects: Juniper Networks Junos OS 14.1X53 versions prior to 14.1X53-D53 on QFX Series; 14.1 versions 14.1R1 and later versions prior to 15.1 versions prior to 15.1R7-S6 on QFX Series, PTX Series; 15.1X53 versions prior to 15.1X53-D593 on QFX Series; 16.1 versions prior to 16.1R7-S7 on QFX Series, PTX Series; 16.2 versions prior to 16.2R2-S11, 16.2R3 on QFX Series, PTX Series; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2 on QFX Series, PTX Series; 17.2 versions prior to 17.2R1-S9, 17.2R3-S3 on QFX Series, PTX Series; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7 on QFX Series, PTX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3 on QFX Series, PTX Series; 18.1 versions prior to 18.1R3-S9 on QFX Series, PTX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on QFX Series, PTX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1 on QFX Series, PTX Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R2-S7, 18.4R3 on QFX Series, PTX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on QFX Series, PTX Series; 19.2 versions prior</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to 19.2R1-S3, 19.2R2 on QFX Series, PTX Series. CVE ID : CVE-2021-0247		
ptx10002-60c					
Uncontrolled Resource Consumption	22-04-2021	5	<p>On Juniper Networks Junos OS platforms with link aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel: rt_pfe_veto: Memory over consumed. Op 1 err 12, rtsm_id 0:-1, msg type 72 /kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd</p> <p>An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Size(s) ifstat 2588977 162708K - 19633958 <<<<</p> <p>user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests</p>	https://kb.juniper.net/JS_A11125	H-JUN-PTX1-040521/572

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<< This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000- 72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3.</p> <p>CVE ID : CVE-2021-0230</p>		

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
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	4.3	On PTX Series and QFX10k Series devices with the "inline-jflow" feature enabled, a use after free weakness in the Packet Forwarding Engine (PFE) microkernel architecture of Juniper Networks Junos OS may allow an attacker to cause a Denial of Service (DoS) condition whereby one or more Flexible PIC Concentrators (FPCs) may restart. As this is a race condition situation this issue become more likely to be hit when network instability occurs, such as but not limited to BGP/IGP reconvergences, and/or further likely to occur when more active "traffic flows" are occurring through the device. When this issue occurs, it will cause one or more FPCs to restart unexpectedly. During FPC restarts core files will be generated. While the core file is generated traffic will be disrupted. Sustained receipt of large traffic flows and reconvergence-like situations may sustain the Denial of Service (DoS) situation. This issue affects: Juniper Networks Junos OS: 18.1 version 18.1R2 and later versions prior to 18.1R3-S10 on PTX Series, QFX10K Series. CVE ID : CVE-2021-0270	https://kb.juniper.net/JS_A11161 , https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/inline-flow-monitoring-ptx.html	H-JUN-PTX1-040521/573
Concurrent	22-04-2021	6.8	A Race Condition	https://kb.juniper.net	H-JUN-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Execution using Shared Resource with Improper Synchronization ('Race Condition')			<p>(Concurrent Execution using Shared Resource with Improper Synchronization) vulnerability in the firewall process (dfwd) of Juniper Networks Junos OS allows an attacker to bypass the firewall rule sets applied to the input loopback filter on any interfaces of a device. This issue is detectable by reviewing the PFE firewall rules, as well as the firewall counters and seeing if they are incrementing or not. For example: show firewall Filter:</p> <pre>__default_bpdu_filter__ Filter: FILTER-INET-01 Counters: Name Bytes Packets output-match-inet 0 0 <<<<<< missing firewall packet count</pre> <p>This issue affects: Juniper Networks Junos OS 14.1X53 versions prior to 14.1X53-D53 on QFX Series; 14.1 versions 14.1R1 and later versions prior to 15.1 versions prior to 15.1R7-S6 on QFX Series, PTX Series; 15.1X53 versions prior to 15.1X53-D593 on QFX Series; 16.1 versions prior to 16.1R7-S7 on QFX Series, PTX Series; 16.2 versions prior to 16.2R2-S11, 16.2R3 on QFX Series, PTX Series; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2 on QFX Series, PTX Series; 17.2 versions prior to 17.2R1-S9, 17.2R3-S3 on QFX Series, PTX Series; 17.3 versions</p>	niper.net/JS A11140	PTX1-040521/574

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>prior to 17.3R2-S5, 17.3R3-S7 on QFX Series, PTX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3 on QFX Series, PTX Series; 18.1 versions prior to 18.1R3-S9 on QFX Series, PTX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on QFX Series, PTX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1 on QFX Series, PTX Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R2-S7, 18.4R3 on QFX Series, PTX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on QFX Series, PTX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on QFX Series, PTX Series.</p> <p>CVE ID : CVE-2021-0247</p>		
Improper Handling of Exceptional Conditions	22-04-2021	5	<p>A vulnerability in the processing of traffic matching a firewall filter containing a syslog action in Juniper Networks Junos OS on MX Series with MPC10/MPC11 cards installed, PTX10003 and PTX10008 Series devices, will cause the line card to crash and restart, creating a Denial of Service (DoS). Continued receipt and processing of packets matching the firewall filter can create a sustained Denial of Service (DoS) condition. When traffic hits the firewall filter, configured on lo0 or any</p>	<p>https://kb.juniper.net/JS_A11155, https://kb.juniper.net/TS_B17931</p>	H-JUN-PTX1-040521/575

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			physical interface on the line card, containing a term with a syslog action (e.g. 'term <name> then syslog'), the affected line card will crash and restart, impacting traffic processing through the ports of the line card. This issue only affects MX Series routers with MPC10 or MPC11 line cards, and PTX10003 or PTX10008 Series packet transport routers. No other platforms or models of line cards are affected by this issue. Note: This issue has also been identified and described in technical service bulletin TSB17931 (login required). This issue affects: Juniper Networks Junos OS on MX Series: 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2. Juniper Networks Junos OS Evolved on PTX10003, PTX10008: All versions prior to 20.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1. CVE ID : CVE-2021-0264							
ptx10003_160c										
Uncontrolled Resource Consumption	22-04-2021	5	On Juniper Networks Junos OS platforms with link aggregation (lag)	https://kb.juniper.net/JS_A11125	H-JUN-PTX1-040521/576					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel: rt_pfe_veto: Memory over consumed. Op 1 err 12, rtsm_id 0:-1, msg type 72 /kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd</p> <p>An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device</p> <pre>> show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<< user@device > show system virtual-memory no- forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<< This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000- 72Q, PTX3000, PTX5000,</pre>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3. CVE ID : CVE-2021-0230		
ptx10003_80c					
Uncontrolled Resource Consumption	22-04-2021	5	On Juniper Networks Junos OS platforms with link aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to	https://kb.juniper.net/JS_A11125	H-JUN-PTX1-040521/577

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>SNMP GET requests, causes a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel: rt_pfe_veto: Memory over consumed. Op 1 err 12, rtsm_id 0:-1, msg type 72 /kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd</p> <p>An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<<</p> <p>user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<< This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000-72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008,</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>PTX10016 Series. Juniper Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3.</p> <p>CVE ID : CVE-2021-0230</p>		
ptx10003_81cd					
Uncontrolled Resource Consumption	22-04-2021	5	<p>On Juniper Networks Junos OS platforms with link aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot</p>	https://kb.juniper.net/JS_A11125	H-JUN-PTX1-040521/578

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>might be required. The following log can be seen if this issue happens. /kernel: rt_pfe_veto: Memory over consumed. Op 1 err 12, rtsm_id 0:-1, msg type 72 /kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd</p> <p>An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958</p> <p><<<<user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<< This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000-72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3.</p> <p>CVE ID : CVE-2021-0230</p>		
ptx10004					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	4.3	<p>On PTX Series and QFX10k Series devices with the "inline-jflow" feature enabled, a use after free weakness in the Packet Forwarding Engine (PFE) microkernel architecture of Juniper Networks Junos OS may allow an attacker to cause a Denial of Service (DoS) condition whereby one or more Flexible PIC Concentrators (FPCs) may restart. As this is a race condition situation this issue become more likely to be hit when network instability occurs, such as</p>	<p>https://kb.juniper.net/JS_A11161, https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/inline-flow-monitoring-ptx.html</p>	H-JUN-PTX1-040521/579

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>but not limited to BGP/IGP reconvergences, and/or further likely to occur when more active "traffic flows" are occurring through the device. When this issue occurs, it will cause one or more FPCs to restart unexpectedly. During FPC restarts core files will be generated. While the core file is generated traffic will be disrupted. Sustained receipt of large traffic flows and reconvergence-like situations may sustain the Denial of Service (DoS) situation. This issue affects: Juniper Networks Junos OS: 18.1 version 18.1R2 and later versions prior to 18.1R3-S10 on PTX Series, QFX10K Series.</p> <p>CVE ID : CVE-2021-0270</p>		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	6.8	<p>A Race Condition (Concurrent Execution using Shared Resource with Improper Synchronization) vulnerability in the firewall process (dfwd) of Juniper Networks Junos OS allows an attacker to bypass the firewall rule sets applied to the input loopback filter on any interfaces of a device. This issue is detectable by reviewing the PFE firewall rules, as well as the firewall counters and seeing if they are incrementing or not. For example: show firewall Filter:</p> <p><code>__default_bpdu_filter__</code></p>	https://kb.juniper.net/JS_A11140	H-JUN-PTX1-040521/580

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Filter: FILTER-INET-01</p> <p>Counters: Name Bytes</p> <p>Packets output-match-inet</p> <p>0 0 <<<<< missing firewall packet count This issue affects: Juniper Networks Junos OS 14.1X53 versions prior to 14.1X53-D53 on QFX Series; 14.1 versions 14.1R1 and later versions prior to 15.1 versions prior to 15.1R7-S6 on QFX Series, PTX Series; 15.1X53 versions prior to 15.1X53-D593 on QFX Series; 16.1 versions prior to 16.1R7-S7 on QFX Series, PTX Series; 16.2 versions prior to 16.2R2-S11, 16.2R3 on QFX Series, PTX Series; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2 on QFX Series, PTX Series; 17.2 versions prior to 17.2R1-S9, 17.2R3-S3 on QFX Series, PTX Series; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7 on QFX Series, PTX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3 on QFX Series, PTX Series; 18.1 versions prior to 18.1R3-S9 on QFX Series, PTX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on QFX Series, PTX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1 on QFX Series, PTX Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R2-S7, 18.4R3 on QFX Series, PTX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1,</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.1R3 on QFX Series, PTX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on QFX Series, PTX Series. CVE ID : CVE-2021-0247		
Uncontrolled Resource Consumption	22-04-2021	5	On Juniper Networks Junos OS platforms with link aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel: rt_pfe_veto: Memory over consumed. Op 1 err 12, rtsm_id 0:-1, msg type 72 /kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<< user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse	https://kb.juniper.net/JS_A11125	H-JUN-PTX1-040521/581

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>HighUse Limit Requests Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<< This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000- 72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3.</p> <p>CVE ID : CVE-2021-0230</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ptx10008					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	4.3	<p>On PTX Series and QFX10k Series devices with the "inline-jflow" feature enabled, a use after free weakness in the Packet Forwarding Engine (PFE) microkernel architecture of Juniper Networks Junos OS may allow an attacker to cause a Denial of Service (DoS) condition whereby one or more Flexible PIC Concentrators (FPCs) may restart. As this is a race condition situation this issue become more likely to be hit when network instability occurs, such as but not limited to BGP/IGP reconvergences, and/or further likely to occur when more active "traffic flows" are occurring through the device. When this issue occurs, it will cause one or more FPCs to restart unexpectedly. During FPC restarts core files will be generated. While the core file is generated traffic will be disrupted. Sustained receipt of large traffic flows and reconvergence-like situations may sustain the Denial of Service (DoS) situation. This issue affects: Juniper Networks Junos OS: 18.1 version 18.1R2 and later versions prior to 18.1R3-S10 on PTX Series, QFX10K Series.</p> <p>CVE ID : CVE-2021-0270</p>	<p>https://kb.juniper.net/JS_A11161, https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/inline-flow-monitoring-ptx.html</p>	H-JUN-PTX1-040521/582

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	6.8	<p>A Race Condition (Concurrent Execution using Shared Resource with Improper Synchronization) vulnerability in the firewall process (dfwd) of Juniper Networks Junos OS allows an attacker to bypass the firewall rule sets applied to the input loopback filter on any interfaces of a device. This issue is detectable by reviewing the PFE firewall rules, as well as the firewall counters and seeing if they are incrementing or not. For example: show firewall Filter:</p> <pre>__default_bpdu_filter__ Filter: FILTER-INET-01 Counters: Name Bytes Packets output-match-inet 0 0 <<<<<< missing firewall packet count</pre> <p>This issue affects: Juniper Networks Junos OS 14.1X53 versions prior to 14.1X53-D53 on QFX Series; 14.1 versions 14.1R1 and later versions prior to 15.1 versions prior to 15.1R7-S6 on QFX Series, PTX Series; 15.1X53 versions prior to 15.1X53-D593 on QFX Series; 16.1 versions prior to 16.1R7-S7 on QFX Series, PTX Series; 16.2 versions prior to 16.2R2-S11, 16.2R3 on QFX Series, PTX Series; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2 on QFX Series, PTX Series; 17.2 versions prior to 17.2R1-S9, 17.2R3-S3 on QFX Series,</p>	https://kb.juniper.net/JS_A11140	H-JUN-PTX1-040521/583

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>PTX Series; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7 on QFX Series, PTX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3 on QFX Series, PTX Series; 18.1 versions prior to 18.1R3-S9 on QFX Series, PTX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on QFX Series, PTX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1 on QFX Series, PTX Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R2-S7, 18.4R3 on QFX Series, PTX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on QFX Series, PTX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on QFX Series, PTX Series.</p> <p>CVE ID : CVE-2021-0247</p>		
Uncontrolled Resource Consumption	22-04-2021	5	<p>On Juniper Networks Junos OS platforms with link aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel: rt_pfe_veto: Memory over consumed. Op 1 err 12, rtshm_id 0:-1, msg type 72</p>	https://kb.juniper.net/JS_A11125	H-JUN-PTX1-040521/584

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>/kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd</p> <p>An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device</p> <pre>> show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<<</pre> <p>user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<<</p> <p>This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000-72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3. CVE ID : CVE-2021-0230		
Improper Handling of Exceptional Conditions	22-04-2021	5	A vulnerability in the processing of traffic matching a firewall filter containing a syslog action in Juniper Networks Junos OS on MX Series with MPC10/MPC11 cards installed, PTX10003 and PTX10008 Series devices, will cause the line card to crash and restart, creating a Denial of Service (DoS). Continued receipt and processing of packets matching the firewall filter can create a sustained Denial of Service (DoS) condition. When traffic hits the firewall filter, configured on lo0 or any physical interface on the line card, containing a term with a syslog action (e.g. 'term <name> then syslog'), the affected line card will	https://kb.juniper.net/JS_A11155 , https://kb.juniper.net/TS_B17931	H-JUN-PTX1-040521/585

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>crash and restart, impacting traffic processing through the ports of the line card. This issue only affects MX Series routers with MPC10 or MPC11 line cards, and PTX10003 or PTX10008 Series packet transport routers. No other platforms or models of line cards are affected by this issue. Note: This issue has also been identified and described in technical service bulletin TSB17931 (login required). This issue affects: Juniper Networks Junos OS on MX Series: 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2. Juniper Networks Junos OS Evolved on PTX10003, PTX10008: All versions prior to 20.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1.</p> <p>CVE ID : CVE-2021-0264</p>		
ptx10016					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race	22-04-2021	4.3	On PTX Series and QFX10k Series devices with the "inline-jflow" feature enabled, a use after free weakness in the Packet Forwarding Engine (PFE) microkernel architecture of Juniper Networks Junos OS	https://kb.juniper.net/JS_A11161 , https://www.juniper.net/documentation/en_US/junos/topic	H-JUN-PTX1-040521/586

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Condition')			<p>may allow an attacker to cause a Denial of Service (DoS) condition whereby one or more Flexible PIC Concentrators (FPCs) may restart. As this is a race condition situation this issue become more likely to be hit when network instability occurs, such as but not limited to BGP/IGP reconvergences, and/or further likely to occur when more active "traffic flows" are occurring through the device. When this issue occurs, it will cause one or more FPCs to restart unexpectedly. During FPC restarts core files will be generated. While the core file is generated traffic will be disrupted. Sustained receipt of large traffic flows and reconvergence-like situations may sustain the Denial of Service (DoS) situation. This issue affects: Juniper Networks Junos OS: 18.1 version 18.1R2 and later versions prior to 18.1R3-S10 on PTX Series, QFX10K Series.</p> <p>CVE ID : CVE-2021-0270</p>	s/task/configuration/inline-flow-monitoring-ptx.html	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	6.8	<p>A Race Condition (Concurrent Execution using Shared Resource with Improper Synchronization) vulnerability in the firewall process (dfwd) of Juniper Networks Junos OS allows an attacker to bypass the firewall rule sets applied to</p>	https://kb.juniper.net/JS_A11140	H-JUN-PTX1-040521/587

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>the input loopback filter on any interfaces of a device. This issue is detectable by reviewing the PFE firewall rules, as well as the firewall counters and seeing if they are incrementing or not. For example: show firewall Filter:</p> <pre>__default_bpdu_filter__ Filter: FILTER-INET-01 Counters: Name Bytes Packets output-match-inet 0 0 <<<<< missing firewall packet count</pre> <p>This issue affects: Juniper Networks Junos OS 14.1X53 versions prior to 14.1X53-D53 on QFX Series; 14.1 versions 14.1R1 and later versions prior to 15.1 versions prior to 15.1R7-S6 on QFX Series, PTX Series; 15.1X53 versions prior to 15.1X53-D593 on QFX Series; 16.1 versions prior to 16.1R7-S7 on QFX Series, PTX Series; 16.2 versions prior to 16.2R2-S11, 16.2R3 on QFX Series, PTX Series; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2 on QFX Series, PTX Series; 17.2 versions prior to 17.2R1-S9, 17.2R3-S3 on QFX Series, PTX Series; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7 on QFX Series, PTX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3 on QFX Series, PTX Series; 18.1 versions prior to 18.1R3-S9 on QFX Series, PTX Series; 18.2 versions prior to</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.2R2-S6, 18.2R3-S3 on QFX Series, PTX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1 on QFX Series, PTX Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R2-S7, 18.4R3 on QFX Series, PTX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on QFX Series, PTX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on QFX Series, PTX Series. CVE ID : CVE-2021-0247		
Uncontrolled Resource Consumption	22-04-2021	5	On Juniper Networks Junos OS platforms with link aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel: rt_pfe_veto: Memory over consumed. Op 1 err 12, rtsm_id 0:-1, msg type 72 /kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device > show system virtual-	https://kb.juniper.net/JS_A11125	H-JUN-PTX1-040521/588

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
			<p>memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<< user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<< This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000-72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1;</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3. CVE ID : CVE-2021-0230		
ptx3000					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	4.3	On PTX Series and QFX10k Series devices with the "inline-jflow" feature enabled, a use after free weakness in the Packet Forwarding Engine (PFE) microkernel architecture of Juniper Networks Junos OS may allow an attacker to cause a Denial of Service (DoS) condition whereby one or more Flexible PIC Concentrators (FPCs) may restart. As this is a race condition situation this issue become more likely to be hit when network instability occurs, such as but not limited to BGP/IGP reconvergences, and/or further likely to occur when more active "traffic flows" are occurring through the device. When this issue occurs, it will cause one or more FPCs to restart unexpectedly. During FPC restarts core files will be generated. While the core file is generated traffic will be disrupted. Sustained receipt of large traffic flows and reconvergence-like	https://kb.juniper.net/JS_A11161 , https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/inline-flow-monitoring-ptx.html	H-JUN-PTX3-040521/589

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>situations may sustain the Denial of Service (DoS) situation. This issue affects: Juniper Networks Junos OS: 18.1 version 18.1R2 and later versions prior to 18.1R3-S10 on PTX Series, QFX10K Series.</p> <p>CVE ID : CVE-2021-0270</p>		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	6.8	<p>A Race Condition (Concurrent Execution using Shared Resource with Improper Synchronization) vulnerability in the firewall process (dfwd) of Juniper Networks Junos OS allows an attacker to bypass the firewall rule sets applied to the input loopback filter on any interfaces of a device. This issue is detectable by reviewing the PFE firewall rules, as well as the firewall counters and seeing if they are incrementing or not. For example: show firewall Filter: <code>_default_bpdu_filter_</code> Filter: FILTER-INET-01 Counters: Name Bytes Packets output-match-inet 0 0 <<<<< missing firewall packet count This issue affects: Juniper Networks Junos OS 14.1X53 versions prior to 14.1X53-D53 on QFX Series; 14.1 versions 14.1R1 and later versions prior to 15.1 versions prior to 15.1R7-S6 on QFX Series, PTX Series; 15.1X53 versions prior to 15.1X53-D593 on QFX Series; 16.1</p>	https://kb.juniper.net/JS_A11140	H-JUN-PTX3-040521/590

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 16.1R7-S7 on QFX Series, PTX Series; 16.2 versions prior to 16.2R2-S11, 16.2R3 on QFX Series, PTX Series; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2 on QFX Series, PTX Series; 17.2 versions prior to 17.2R1-S9, 17.2R3-S3 on QFX Series, PTX Series; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7 on QFX Series, PTX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3 on QFX Series, PTX Series; 18.1 versions prior to 18.1R3-S9 on QFX Series, PTX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on QFX Series, PTX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1 on QFX Series, PTX Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R2-S7, 18.4R3 on QFX Series, PTX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on QFX Series, PTX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on QFX Series, PTX Series. CVE ID : CVE-2021-0247		
Uncontrolled Resource Consumption	22-04-2021	5	On Juniper Networks Junos OS platforms with link aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes	https://kb.juniper.net/JS_A11125	H-JUN-PTX3-040521/591

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel: rt_pfe_veto: Memory over consumed. Op 1 err 12, rtsm_id 0:-1, msg type 72 /kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd</p> <p>An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<<</p> <p>user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<< This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000-72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3.</p> <p>CVE ID : CVE-2021-0230</p>		
ptx5000					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	4.3	<p>On PTX Series and QFX10k Series devices with the "inline-jflow" feature enabled, a use after free weakness in the Packet Forwarding Engine (PFE) microkernel architecture of Juniper Networks Junos OS may allow an attacker to cause a Denial of Service (DoS) condition whereby one or more Flexible PIC Concentrators (FPCs) may restart. As this is a race</p>	https://kb.juniper.net/JS_A11161 , https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/inline-flow-monitoring-ptx.html	H-JUN-PTX5-040521/592

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>condition situation this issue become more likely to be hit when network instability occurs, such as but not limited to BGP/IGP reconvergences, and/or further likely to occur when more active "traffic flows" are occurring through the device. When this issue occurs, it will cause one or more FPCs to restart unexpectedly. During FPC restarts core files will be generated. While the core file is generated traffic will be disrupted. Sustained receipt of large traffic flows and reconvergence-like situations may sustain the Denial of Service (DoS) situation. This issue affects: Juniper Networks Junos OS: 18.1 version 18.1R2 and later versions prior to 18.1R3-S10 on PTX Series, QFX10K Series.</p> <p>CVE ID : CVE-2021-0270</p>		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	6.8	<p>A Race Condition (Concurrent Execution using Shared Resource with Improper Synchronization) vulnerability in the firewall process (dfwd) of Juniper Networks Junos OS allows an attacker to bypass the firewall rule sets applied to the input loopback filter on any interfaces of a device. This issue is detectable by reviewing the PFE firewall rules, as well as the firewall counters and seeing if they</p>	https://kb.juniper.net/JS_A11140	H-JUN-PTX5-040521/593

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>are incrementing or not. For example: show firewall Filter:</p> <p><code>__default_bpdu_filter__</code></p> <p>Filter: FILTER-INET-01</p> <p>Counters: Name Bytes</p> <p>Packets output-match-inet</p> <p>0 0 <<<<< missing firewall packet count This issue affects: Juniper Networks Junos OS 14.1X53 versions prior to 14.1X53-D53 on QFX Series; 14.1 versions 14.1R1 and later versions prior to 15.1 versions prior to 15.1R7-S6 on QFX Series, PTX Series; 15.1X53 versions prior to 15.1X53-D593 on QFX Series; 16.1 versions prior to 16.1R7-S7 on QFX Series, PTX Series; 16.2 versions prior to 16.2R2-S11, 16.2R3 on QFX Series, PTX Series; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2 on QFX Series, PTX Series; 17.2 versions prior to 17.2R1-S9, 17.2R3-S3 on QFX Series, PTX Series; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7 on QFX Series, PTX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3 on QFX Series, PTX Series; 18.1 versions prior to 18.1R3-S9 on QFX Series, PTX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on QFX Series, PTX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1 on QFX Series, PTX Series; 18.4 versions prior to 18.4R1-S5,</p>		

CVSS Scoring Scale	0-1	1-2	2-3	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-S3, 18.4R2-S7, 18.4R3 on QFX Series, PTX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on QFX Series, PTX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on QFX Series, PTX Series. CVE ID : CVE-2021-0247		
Uncontrolled Resource Consumption	22-04-2021	5	On Juniper Networks Junos OS platforms with link aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak. If all the available memory is consumed, the traffic will be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel: rt_pfe_veto: Memory over consumed. Op 1 err 12, rtsm_id 0:-1, msg type 72 /kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<<	https://kb.juniper.net/JS_A11125	H-JUN-PTX5-040521/594

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<< This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000-72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper Networks EX9200 Series. Juniper Networks ACX710, ACX6360 Series. Juniper Networks NFX Series. This issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper</p>		

CVSS Scoring Scale	0-1	1-2	2-3	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 prior to 17.1R3. CVE ID : CVE-2021-0230		
qfx10002					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	4.3	On PTX Series and QFX10k Series devices with the "inline-jflow" feature enabled, a use after free weakness in the Packet Forwarding Engine (PFE) microkernel architecture of Juniper Networks Junos OS may allow an attacker to cause a Denial of Service (DoS) condition whereby one or more Flexible PIC Concentrators (FPCs) may restart. As this is a race condition situation this issue become more likely to be hit when network instability occurs, such as but not limited to BGP/IGP reconvergences, and/or further likely to occur when more active "traffic flows" are occurring through the device. When this issue occurs, it will cause one or more FPCs to restart unexpectedly. During FPC restarts core files will be generated. While the core file is generated traffic will be disrupted. Sustained receipt of large traffic flows and reconvergence-like situations may sustain the Denial of Service (DoS) situation. This issue affects: Juniper Networks Junos OS: 18.1 version 18.1R2 and later versions prior to	https://kb.juniper.net/JS_A11161 , https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/inline-flow-monitoring-ptx.html	H-JUN-QFX1-040521/595

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.1R3-S10 on PTX Series, QFX10K Series. CVE ID : CVE-2021-0270		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	6.8	A Race Condition (Concurrent Execution using Shared Resource with Improper Synchronization) vulnerability in the firewall process (dfwd) of Juniper Networks Junos OS allows an attacker to bypass the firewall rule sets applied to the input loopback filter on any interfaces of a device. This issue is detectable by reviewing the PFE firewall rules, as well as the firewall counters and seeing if they are incrementing or not. For example: show firewall Filter: __default_bpdu_filter__ Filter: FILTER-INET-01 Counters: Name Bytes Packets output-match-inet 0 0 <<<<< missing firewall packet count This issue affects: Juniper Networks Junos OS 14.1X53 versions prior to 14.1X53-D53 on QFX Series; 14.1 versions 14.1R1 and later versions prior to 15.1 versions prior to 15.1R7-S6 on QFX Series, PTX Series; 15.1X53 versions prior to 15.1X53-D593 on QFX Series; 16.1 versions prior to 16.1R7-S7 on QFX Series, PTX Series; 16.2 versions prior to 16.2R2-S11, 16.2R3 on QFX Series, PTX Series; 17.1 versions prior to 17.1R2-	https://kb.juniper.net/JS_A11140	H-JUN-QFX1-040521/596

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>S11, 17.1R3-S2 on QFX Series, PTX Series; 17.2 versions prior to 17.2R1-S9, 17.2R3-S3 on QFX Series, PTX Series; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7 on QFX Series, PTX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3 on QFX Series, PTX Series; 18.1 versions prior to 18.1R3-S9 on QFX Series, PTX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on QFX Series, PTX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1 on QFX Series, PTX Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R2-S7, 18.4R3 on QFX Series, PTX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on QFX Series, PTX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on QFX Series, PTX Series.</p> <p>CVE ID : CVE-2021-0247</p>		
qfx10008					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	4.3	<p>On PTX Series and QFX10k Series devices with the "inline-jflow" feature enabled, a use after free weakness in the Packet Forwarding Engine (PFE) microkernel architecture of Juniper Networks Junos OS may allow an attacker to cause a Denial of Service (DoS) condition whereby one or more Flexible PIC Concentrators (FPCs) may restart. As this is a race</p>	<p>https://kb.juniper.net/JS_A11161, https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/inline-flow-monitoring-ptx.html</p>	H-JUN-QFX1-040521/597

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>condition situation this issue become more likely to be hit when network instability occurs, such as but not limited to BGP/IGP reconvergences, and/or further likely to occur when more active "traffic flows" are occurring through the device. When this issue occurs, it will cause one or more FPCs to restart unexpectedly. During FPC restarts core files will be generated. While the core file is generated traffic will be disrupted. Sustained receipt of large traffic flows and reconvergence-like situations may sustain the Denial of Service (DoS) situation. This issue affects: Juniper Networks Junos OS: 18.1 version 18.1R2 and later versions prior to 18.1R3-S10 on PTX Series, QFX10K Series.</p> <p>CVE ID : CVE-2021-0270</p>		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	6.8	<p>A Race Condition (Concurrent Execution using Shared Resource with Improper Synchronization) vulnerability in the firewall process (dfwd) of Juniper Networks Junos OS allows an attacker to bypass the firewall rule sets applied to the input loopback filter on any interfaces of a device. This issue is detectable by reviewing the PFE firewall rules, as well as the firewall counters and seeing if they</p>	https://kb.juniper.net/JS_A11140	H-JUN-QFX1-040521/598

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>are incrementing or not. For example: show firewall Filter:</p> <p><code>__default_bpdu_filter__</code></p> <p>Filter: FILTER-INET-01</p> <p>Counters: Name Bytes</p> <p>Packets output-match-inet</p> <p>0 0 <<<<< missing firewall packet count This issue affects: Juniper Networks Junos OS 14.1X53 versions prior to 14.1X53-D53 on QFX Series; 14.1 versions 14.1R1 and later versions prior to 15.1 versions prior to 15.1R7-S6 on QFX Series, PTX Series; 15.1X53 versions prior to 15.1X53-D593 on QFX Series; 16.1 versions prior to 16.1R7-S7 on QFX Series, PTX Series; 16.2 versions prior to 16.2R2-S11, 16.2R3 on QFX Series, PTX Series; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2 on QFX Series, PTX Series; 17.2 versions prior to 17.2R1-S9, 17.2R3-S3 on QFX Series, PTX Series; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7 on QFX Series, PTX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3 on QFX Series, PTX Series; 18.1 versions prior to 18.1R3-S9 on QFX Series, PTX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on QFX Series, PTX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1 on QFX Series, PTX Series; 18.4 versions prior to 18.4R1-S5,</p>		

CVSS Scoring Scale	0-1	1-2	2-3	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-S3, 18.4R2-S7, 18.4R3 on QFX Series, PTX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on QFX Series, PTX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on QFX Series, PTX Series. CVE ID : CVE-2021-0247		
qfx10016					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	4.3	On PTX Series and QFX10k Series devices with the "inline-jflow" feature enabled, a use after free weakness in the Packet Forwarding Engine (PFE) microkernel architecture of Juniper Networks Junos OS may allow an attacker to cause a Denial of Service (DoS) condition whereby one or more Flexible PIC Concentrators (FPCs) may restart. As this is a race condition situation this issue become more likely to be hit when network instability occurs, such as but not limited to BGP/IGP reconvergences, and/or further likely to occur when more active "traffic flows" are occurring through the device. When this issue occurs, it will cause one or more FPCs to restart unexpectedly. During FPC restarts core files will be generated. While the core file is generated traffic will be disrupted. Sustained receipt of large traffic flows and reconvergence-like	https://kb.juniper.net/JS_A11161 , https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/inline-flow-monitoring-ptx.html	H-JUN-QFX1-040521/599

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>situations may sustain the Denial of Service (DoS) situation. This issue affects: Juniper Networks Junos OS: 18.1 version 18.1R2 and later versions prior to 18.1R3-S10 on PTX Series, QFX10K Series.</p> <p>CVE ID : CVE-2021-0270</p>		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	6.8	<p>A Race Condition (Concurrent Execution using Shared Resource with Improper Synchronization) vulnerability in the firewall process (dfwd) of Juniper Networks Junos OS allows an attacker to bypass the firewall rule sets applied to the input loopback filter on any interfaces of a device. This issue is detectable by reviewing the PFE firewall rules, as well as the firewall counters and seeing if they are incrementing or not. For example: show firewall Filter: <code>_default_bpdu_filter_</code> Filter: FILTER-INET-01 Counters: Name Bytes Packets output-match-inet 0 0 <<<<< missing firewall packet count This issue affects: Juniper Networks Junos OS 14.1X53 versions prior to 14.1X53-D53 on QFX Series; 14.1 versions 14.1R1 and later versions prior to 15.1 versions prior to 15.1R7-S6 on QFX Series, PTX Series; 15.1X53 versions prior to 15.1X53-D593 on QFX Series; 16.1</p>	https://kb.juniper.net/JS_A11140	H-JUN-QFX1-040521/600

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 16.1R7-S7 on QFX Series, PTX Series; 16.2 versions prior to 16.2R2-S11, 16.2R3 on QFX Series, PTX Series; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2 on QFX Series, PTX Series; 17.2 versions prior to 17.2R1-S9, 17.2R3-S3 on QFX Series, PTX Series; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7 on QFX Series, PTX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3 on QFX Series, PTX Series; 18.1 versions prior to 18.1R3-S9 on QFX Series, PTX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on QFX Series, PTX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1 on QFX Series, PTX Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R2-S7, 18.4R3 on QFX Series, PTX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on QFX Series, PTX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on QFX Series, PTX Series. CVE ID : CVE-2021-0247		
qfx5100					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race	22-04-2021	6.8	A Race Condition (Concurrent Execution using Shared Resource with Improper Synchronization) vulnerability in the firewall process (dfwd) of Juniper Networks Junos OS allows an attacker to bypass the	https://kb.juniper.net/JS_A11140	H-JUN-QFX5-040521/601

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Condition')			<p>firewall rule sets applied to the input loopback filter on any interfaces of a device. This issue is detectable by reviewing the PFE firewall rules, as well as the firewall counters and seeing if they are incrementing or not. For example: show firewall Filter:</p> <pre>__default_bpdu_filter__ Filter: FILTER-INET-01 Counters: Name Bytes Packets output-match-inet 0 0 <<<<<< missing firewall packet count</pre> <p>This issue affects: Juniper Networks Junos OS 14.1X53 versions prior to 14.1X53-D53 on QFX Series; 14.1 versions 14.1R1 and later versions prior to 15.1 versions prior to 15.1R7-S6 on QFX Series, PTX Series; 15.1X53 versions prior to 15.1X53-D593 on QFX Series; 16.1 versions prior to 16.1R7-S7 on QFX Series, PTX Series; 16.2 versions prior to 16.2R2-S11, 16.2R3 on QFX Series, PTX Series; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2 on QFX Series, PTX Series; 17.2 versions prior to 17.2R1-S9, 17.2R3-S3 on QFX Series, PTX Series; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7 on QFX Series, PTX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3 on QFX Series, PTX Series; 18.1 versions prior to 18.1R3-S9 on QFX Series, PTX Series;</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on QFX Series, PTX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1 on QFX Series, PTX Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R2-S7, 18.4R3 on QFX Series, PTX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on QFX Series, PTX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on QFX Series, PTX Series. CVE ID : CVE-2021-0247		
N/A	22-04-2021	5	On Juniper Networks EX4300-MP Series, EX4600 Series, EX4650 Series, QFX5K Series deployed as a Virtual Chassis with a specific Layer 2 circuit configuration, Packet Forwarding Engine manager (FXPC) process may crash and restart upon receipt of specific layer 2 frames. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP Series, EX4600 Series, EX4650 Series, QFX5K Series 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4, 17.4R3-S5; 18.2 versions prior to 18.2R3-S8; 18.3 versions	https://kb.juniper.net/JS_A11132	H-JUN-QFX5-040521/602

CVSS Scoring Scale	0-1	1-2	2-3	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 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2; CVE ID : CVE-2021-0237		
qfx5100-96s					
Improper Initialization	22-04-2021	5	Due to an improper Initialization vulnerability on Juniper Networks Junos OS QFX5100-96S devices with QFX 5e Series image installed, ddos-protection configuration changes will not take effect beyond the default DDoS (Distributed Denial of Service) settings when configured from the CLI. The DDoS protection (jddosd) daemon allows the device to continue to function while protecting the packet forwarding engine (PFE) during the DDoS attack. When this issue occurs, the default DDoS settings within the PFE apply, as CPU bound packets will be throttled and dropped in the PFE when the limits are exceeded. To check if the device has this issue, the administrator can execute the following command to	https://kb.juniper.net/JS_A11129	H-JUN-QFX5-040521/603

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>monitor the status of DDoS protection: user@device> show ddos-protection protocols error: the ddos-protection subsystem is not running This issue affects only QFX5100-96S devices. No other products or platforms are affected by this issue. This issue affects: Juniper Networks Junos OS on QFX5100-96S: 17.3 versions prior to 17.3R3-S10; 17.4 versions prior to 17.4R3-S4; 18.1 versions prior to 18.1R3-S10; 18.2 versions prior to 18.2R3-S3; 18.3 versions prior to 18.3R3-S2; 18.4 versions prior to 18.4R2-S4, 18.4R3-S1; 19.1 versions prior to 19.1R3, 19.1R3-S4; 19.2 versions prior to 19.2R2; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2;</p> <p>CVE ID : CVE-2021-0234</p>		
qfx5110					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	6.8	<p>A Race Condition (Concurrent Execution using Shared Resource with Improper Synchronization) vulnerability in the firewall process (dfwd) of Juniper Networks Junos OS allows an attacker to bypass the firewall rule sets applied to the input loopback filter on any interfaces of a device. This issue is detectable by reviewing the PFE firewall rules, as well as the firewall counters and seeing if they</p>	https://kb.juniper.net/JS_A11140	H-JUN-QFX5-040521/604

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>are incrementing or not. For example: show firewall Filter:</p> <p><code>__default_bpdu_filter__</code></p> <p>Filter: FILTER-INET-01</p> <p>Counters: Name Bytes</p> <p>Packets output-match-inet</p> <p>0 0 <<<<< missing firewall packet count This issue affects: Juniper Networks Junos OS 14.1X53 versions prior to 14.1X53-D53 on QFX Series; 14.1 versions 14.1R1 and later versions prior to 15.1 versions prior to 15.1R7-S6 on QFX Series, PTX Series; 15.1X53 versions prior to 15.1X53-D593 on QFX Series; 16.1 versions prior to 16.1R7-S7 on QFX Series, PTX Series; 16.2 versions prior to 16.2R2-S11, 16.2R3 on QFX Series, PTX Series; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2 on QFX Series, PTX Series; 17.2 versions prior to 17.2R1-S9, 17.2R3-S3 on QFX Series, PTX Series; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7 on QFX Series, PTX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3 on QFX Series, PTX Series; 18.1 versions prior to 18.1R3-S9 on QFX Series, PTX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on QFX Series, PTX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1 on QFX Series, PTX Series; 18.4 versions prior to 18.4R1-S5,</p>		

CVSS Scoring Scale	0-1	1-2	2-3	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-S3, 18.4R2-S7, 18.4R3 on QFX Series, PTX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on QFX Series, PTX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on QFX Series, PTX Series. CVE ID : CVE-2021-0247		
N/A	22-04-2021	5	On Juniper Networks EX4300-MP Series, EX4600 Series, EX4650 Series, QFX5K Series deployed as a Virtual Chassis with a specific Layer 2 circuit configuration, Packet Forwarding Engine manager (FXPC) process may crash and restart upon receipt of specific layer 2 frames. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP Series, EX4600 Series, EX4650 Series, QFX5K Series 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4, 17.4R3-S5; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4	https://kb.juniper.net/JS_A11132	H-JUN-QFX5-040521/605

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2; CVE ID : CVE-2021-0237		
qfx5120					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	6.8	A Race Condition (Concurrent Execution using Shared Resource with Improper Synchronization) vulnerability in the firewall process (dfwd) of Juniper Networks Junos OS allows an attacker to bypass the firewall rule sets applied to the input loopback filter on any interfaces of a device. This issue is detectable by reviewing the PFE firewall rules, as well as the firewall counters and seeing if they are incrementing or not. For example: show firewall Filter: <code>_default_bpdu_filter_</code> Filter: FILTER-INET-01 Counters: Name Bytes Packets output-match-inet 0 0 <<<<<< missing firewall packet count This issue affects: Juniper Networks Junos OS 14.1X53 versions prior to 14.1X53-D53 on QFX Series; 14.1 versions 14.1R1 and later versions prior to 15.1 versions prior to 15.1R7-S6 on QFX Series, PTX Series; 15.1X53 versions prior to 15.1X53-D593 on QFX Series; 16.1 versions prior to 16.1R7-S7	https://kb.juniper.net/JS_A11140	H-JUN-QFX5-040521/606

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>on QFX Series, PTX Series; 16.2 versions prior to 16.2R2-S11, 16.2R3 on QFX Series, PTX Series; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2 on QFX Series, PTX Series; 17.2 versions prior to 17.2R1-S9, 17.2R3-S3 on QFX Series, PTX Series; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7 on QFX Series, PTX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3 on QFX Series, PTX Series; 18.1 versions prior to 18.1R3-S9 on QFX Series, PTX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on QFX Series, PTX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1 on QFX Series, PTX Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R2-S7, 18.4R3 on QFX Series, PTX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on QFX Series, PTX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on QFX Series, PTX Series.</p> <p>CVE ID : CVE-2021-0247</p>		
N/A	22-04-2021	5	<p>On Juniper Networks EX4300-MP Series, EX4600 Series, EX4650 Series, QFX5K Series deployed as a Virtual Chassis with a specific Layer 2 circuit configuration, Packet Forwarding Engine manager (FXPC) process may crash and restart upon</p>	https://kb.juniper.net/JS_A11132	H-JUN-QFX5-040521/607

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>receipt of specific layer 2 frames. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP Series, EX4600 Series, EX4650 Series, QFX5K Series 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4, 17.4R3-S5; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2;</p> <p>CVE ID : CVE-2021-0237</p>		
qfx5130					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	6.8	<p>A Race Condition (Concurrent Execution using Shared Resource with Improper Synchronization) vulnerability in the firewall process (dfwd) of Juniper Networks Junos OS allows an attacker to bypass the firewall rule sets applied to the input loopback filter on any interfaces of a device.</p>	https://kb.juniper.net/JS_A11140	H-JUN-QFX5-040521/608

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>This issue is detectable by reviewing the PFE firewall rules, as well as the firewall counters and seeing if they are incrementing or not. For example: show firewall Filter:</p> <p><code>_default_bpdu_filter_</code></p> <p>Filter: FILTER-INET-01</p> <p>Counters: Name Bytes</p> <p>Packets output-match-inet</p> <p>0 0 <<<<< missing firewall packet count</p> <p>This issue affects: Juniper Networks Junos OS 14.1X53 versions prior to 14.1X53-D53 on QFX Series; 14.1 versions 14.1R1 and later versions prior to 15.1 versions prior to 15.1R7-S6 on QFX Series, PTX Series; 15.1X53 versions prior to 15.1X53-D593 on QFX Series; 16.1 versions prior to 16.1R7-S7 on QFX Series, PTX Series; 16.2 versions prior to 16.2R2-S11, 16.2R3 on QFX Series, PTX Series; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2 on QFX Series, PTX Series; 17.2 versions prior to 17.2R1-S9, 17.2R3-S3 on QFX Series, PTX Series; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7 on QFX Series, PTX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3 on QFX Series, PTX Series; 18.1 versions prior to 18.1R3-S9 on QFX Series, PTX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on QFX Series, PTX Series; 18.3</p>		

CVSS Scoring Scale	0-1	1-2	2-3	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 QFX Series, PTX Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R2-S7, 18.4R3 on QFX Series, PTX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on QFX Series, PTX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on QFX Series, PTX Series. CVE ID : CVE-2021-0247		
N/A	22-04-2021	5	On Juniper Networks EX4300-MP Series, EX4600 Series, EX4650 Series, QFX5K Series deployed as a Virtual Chassis with a specific Layer 2 circuit configuration, Packet Forwarding Engine manager (FXPC) process may crash and restart upon receipt of specific layer 2 frames. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP Series, EX4600 Series, EX4650 Series, QFX5K Series 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4, 17.4R3-S5; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions	https://kb.juniper.net/JS_A11132	H-JUN-QFX5-040521/609

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2;</p> <p>CVE ID : CVE-2021-0237</p>		
qfx5200					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	6.8	<p>A Race Condition (Concurrent Execution using Shared Resource with Improper Synchronization) vulnerability in the firewall process (dfwd) of Juniper Networks Junos OS allows an attacker to bypass the firewall rule sets applied to the input loopback filter on any interfaces of a device. This issue is detectable by reviewing the PFE firewall rules, as well as the firewall counters and seeing if they are incrementing or not. For example: show firewall Filter:</p> <pre>__default_bpdu_filter__ Filter: FILTER-INET-01 Counters: Name Bytes Packets output-match-inet 0 0 <<<<<< missing firewall packet count</pre> <p>This issue affects: Juniper Networks Junos OS 14.1X53 versions prior to 14.1X53-D53 on QFX Series; 14.1 versions 14.1R1 and later versions prior to 15.1 versions prior to 15.1R7-S6 on QFX Series,</p>	https://kb.juniper.net/JS_A11140	H-JUN-QFX5-040521/610

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PTX Series; 15.1X53 versions prior to 15.1X53-D593 on QFX Series; 16.1 versions prior to 16.1R7-S7 on QFX Series, PTX Series; 16.2 versions prior to 16.2R2-S11, 16.2R3 on QFX Series, PTX Series; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2 on QFX Series, PTX Series; 17.2 versions prior to 17.2R1-S9, 17.2R3-S3 on QFX Series, PTX Series; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7 on QFX Series, PTX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3 on QFX Series, PTX Series; 18.1 versions prior to 18.1R3-S9 on QFX Series, PTX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on QFX Series, PTX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1 on QFX Series, PTX Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R2-S7, 18.4R3 on QFX Series, PTX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on QFX Series, PTX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on QFX Series, PTX Series. CVE ID : CVE-2021-0247		
N/A	22-04-2021	5	On Juniper Networks EX4300-MP Series, EX4600 Series, EX4650 Series, QFX5K Series deployed as a Virtual Chassis with a specific Layer 2 circuit	https://kb.juniper.net/JS_A11132	H-JUN-QFX5-040521/611

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			configuration, Packet Forwarding Engine manager (FXPC) process may crash and restart upon receipt of specific layer 2 frames. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP Series, EX4600 Series, EX4650 Series, QFX5K Series 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4, 17.4R3-S5; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2; CVE ID : CVE-2021-0237		
qfx5210					
Concurrent Execution using Shared Resource with Improper Synchronizati	22-04-2021	6.8	A Race Condition (Concurrent Execution using Shared Resource with Improper Synchronization) vulnerability in the firewall process (dfwd) of Juniper Networks Junos OS allows	https://kb.juniper.net/JS_A11140	H-JUN-QFX5-040521/612

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on ('Race Condition')			<p>an attacker to bypass the firewall rule sets applied to the input loopback filter on any interfaces of a device. This issue is detectable by reviewing the PFE firewall rules, as well as the firewall counters and seeing if they are incrementing or not. For example: show firewall Filter:</p> <pre>__default_bpdu_filter__ Filter: FILTER-INET-01 Counters: Name Bytes Packets output-match-inet 0 0 <<<<< missing firewall packet count</pre> <p>This issue affects: Juniper Networks Junos OS 14.1X53 versions prior to 14.1X53-D53 on QFX Series; 14.1 versions 14.1R1 and later versions prior to 15.1 versions prior to 15.1R7-S6 on QFX Series, PTX Series; 15.1X53 versions prior to 15.1X53-D593 on QFX Series; 16.1 versions prior to 16.1R7-S7 on QFX Series, PTX Series; 16.2 versions prior to 16.2R2-S11, 16.2R3 on QFX Series, PTX Series; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2 on QFX Series, PTX Series; 17.2 versions prior to 17.2R1-S9, 17.2R3-S3 on QFX Series, PTX Series; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7 on QFX Series, PTX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3 on QFX Series, PTX Series; 18.1 versions prior to 18.1R3-S9</p>		

CVSS Scoring Scale	0-1	1-2	2-3	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 QFX Series, PTX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on QFX Series, PTX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1 on QFX Series, PTX Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R2-S7, 18.4R3 on QFX Series, PTX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on QFX Series, PTX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on QFX Series, PTX Series. CVE ID : CVE-2021-0247		
N/A	22-04-2021	5	On Juniper Networks EX4300-MP Series, EX4600 Series, EX4650 Series, QFX5K Series deployed as a Virtual Chassis with a specific Layer 2 circuit configuration, Packet Forwarding Engine manager (FXPC) process may crash and restart upon receipt of specific layer 2 frames. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP Series, EX4600 Series, EX4650 Series, QFX5K Series 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4, 17.4R3-S5; 18.2 versions prior to	https://kb.juniper.net/JS_A11132	H-JUN-QFX5-040521/613

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2; CVE ID : CVE-2021-0237		
qfx5220					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	6.8	A Race Condition (Concurrent Execution using Shared Resource with Improper Synchronization) vulnerability in the firewall process (dfwd) of Juniper Networks Junos OS allows an attacker to bypass the firewall rule sets applied to the input loopback filter on any interfaces of a device. This issue is detectable by reviewing the PFE firewall rules, as well as the firewall counters and seeing if they are incrementing or not. For example: show firewall Filter: _default_bpdu_filter_ Filter: FILTER-INET-01 Counters: Name Bytes Packets output-match-inet 0 0 <<<<<< missing firewall packet count This issue affects: Juniper Networks Junos OS 14.1X53 versions prior to 14.1X53-D53 on	https://kb.juniper.net/JS_A11140	H-JUN-QFX5-040521/614

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>QFX Series; 14.1 versions 14.1R1 and later versions prior to 15.1 versions prior to 15.1R7-S6 on QFX Series, PTX Series; 15.1X53 versions prior to 15.1X53-D593 on QFX Series; 16.1 versions prior to 16.1R7-S7 on QFX Series, PTX Series; 16.2 versions prior to 16.2R2-S11, 16.2R3 on QFX Series, PTX Series; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2 on QFX Series, PTX Series; 17.2 versions prior to 17.2R1-S9, 17.2R3-S3 on QFX Series, PTX Series; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7 on QFX Series, PTX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3 on QFX Series, PTX Series; 18.1 versions prior to 18.1R3-S9 on QFX Series, PTX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on QFX Series, PTX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1 on QFX Series, PTX Series; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R2-S7, 18.4R3 on QFX Series, PTX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on QFX Series, PTX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on QFX Series, PTX Series.</p> <p>CVE ID : CVE-2021-0247</p>		
N/A	22-04-2021	5	On Juniper Networks EX4300-MP Series, EX4600	https://kb.juniper.net/JS	H-JUN-QFX5-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Series, EX4650 Series, QFX5K Series deployed as a Virtual Chassis with a specific Layer 2 circuit configuration, Packet Forwarding Engine manager (FXPC) process may crash and restart upon receipt of specific layer 2 frames. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX4300-MP Series, EX4600 Series, EX4650 Series, QFX5K Series 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4, 17.4R3-S5; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2; CVE ID : CVE-2021-0237	A11132	040521/615					
srx100										
Improper Restriction of Operations	22-04-2021	5	An improper restriction of operations within the bounds of a memory buffer	https://kb.juniper.net/JS_A11122	H-JUN-SRX1-040521/616					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
within the Bounds of a Memory Buffer			vulnerability in Juniper Networks Junos OS J-Web on SRX Series devices allows an attacker to cause Denial of Service (DoS) by sending certain crafted HTTP packets. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. When this issue occurs, web-management, NTP daemon (ntpd) and Layer 2 Control Protocol process (L2CPD) daemons might crash. This issue affects Juniper Networks Junos OS on SRX Series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2; CVE ID : CVE-2021-0227							
srx110										
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-04-2021	5	An improper restriction of operations within the bounds of a memory buffer vulnerability in Juniper Networks Junos OS J-Web on SRX Series devices allows an attacker to cause	https://kb.juniper.net/JS_A11122	H-JUN-SRX1-040521/617					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Denial of Service (DoS) by sending certain crafted HTTP packets. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. When this issue occurs, web-management, NTP daemon (ntpd) and Layer 2 Control Protocol process (L2CPD) daemons might crash. This issue affects Juniper Networks Junos OS on SRX Series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2; CVE ID : CVE-2021-0227		
srx1400					
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-04-2021	5	An improper restriction of operations within the bounds of a memory buffer vulnerability in Juniper Networks Junos OS J-Web on SRX Series devices allows an attacker to cause Denial of Service (DoS) by sending certain crafted HTTP packets. Continued receipt and processing of	https://kb.juniper.net/JS_A11122	H-JUN-SRX1-040521/618

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			these packets will create a sustained Denial of Service (DoS) condition. When this issue occurs, web-management, NTP daemon (ntpd) and Layer 2 Control Protocol process (L2CPD) daemons might crash. This issue affects Juniper Networks Junos OS on SRX Series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2; CVE ID : CVE-2021-0227		
srx1500					
Incorrect Default Permissions	22-04-2021	4.6	On SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3, vSRX Series devices using tenant services on Juniper Networks Junos OS, due to incorrect permission scheme assigned to tenant system administrators, a tenant system administrator may inadvertently send their network traffic to one or more tenants while	https://kb.juniper.net/JS_A11130	H-JUN-SRX1-040521/619

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>concurrently modifying the overall device system traffic management, affecting all tenants and the service provider. Further, a tenant may inadvertently receive traffic from another tenant. This issue affects: Juniper Networks Junos OS 18.3 version 18.3R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2; 18.4 version 18.4R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.1 versions 19.1R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.3 versions prior to 19.3R3-S2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 20.1 versions prior to 20.1R2, 20.1R3 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series;</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>20.2 versions prior to 20.2R2-S1, 20.2R3 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series;</p> <p>20.3 versions prior to 20.3R1-S2, 20.3R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series;</p> <p>20.4 versions prior to 20.4R1, 20.4R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series.</p> <p>This issue does not affect Juniper Networks Junos OS versions prior to 18.3R1.</p> <p>CVE ID : CVE-2021-0235</p>		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-04-2021	10	<p>On SRX Series devices configured with UTM services a buffer overflow vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS may allow an attacker to arbitrarily execute code or commands on the target to take over or otherwise impact the device by sending crafted packets to or through the device. This issue affects: Juniper Networks Junos OS on SRX Series: 15.1X49 versions prior to 15.1X49-D190; 17.4 versions prior to 17.4R2-S9; 17.4R3 and later versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S1;</p>	https://kb.juniper.net/JS_A11142	H-JUN-SRX1-040521/620

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.3 versions prior to 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R2-S3, 18.4R3; 19.1 versions prior to 19.1R1-S4, 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. An indicator of compromise can be the following text in the UTM log: RT_UTM: AV_FILE_NOT_SCANNED_PASSED_MT: CVE ID : CVE-2021-0249		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-04-2021	5	An improper restriction of operations within the bounds of a memory buffer vulnerability in Juniper Networks Junos OS J-Web on SRX Series devices allows an attacker to cause Denial of Service (DoS) by sending certain crafted HTTP packets. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. When this issue occurs, web-management, NTP daemon (ntpd) and Layer 2 Control Protocol process (L2CPD) daemons might crash. This issue affects Juniper Networks Junos OS on SRX Series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to	https://kb.juniper.net/JS_A11122	H-JUN-SRX1-040521/621

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2; CVE ID : CVE-2021-0227		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	4.3	A signal handler race condition exists in the Layer 2 Address Learning Daemon (L2ALD) of Juniper Networks Junos OS due to the absence of a specific protection mechanism to avoid a race condition which may allow an attacker to bypass the storm-control feature on devices. This issue is a corner case and only occurs during specific actions taken by an administrator of a device under certain specific actions which triggers the event. The event occurs less frequently on devices which are not configured with Virtual Chassis configurations, and more frequently on devices configured in Virtual Chassis configurations. This issue is not specific to any particular Junos OS platform. An Indicator of Compromise (IoC) may be seen by reviewing log files for the following error message seen by executing the following show statement: show log messages grep storm	https://kb.juniper.net/JS_A11137	H-JUN-SRX1-040521/622

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Result to look for: /kernel: GENCFG: op 58 (Storm Control Blob) failed; err 1 (Unknown) This issue affects: Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D49 on EX Series; 15.1 versions prior to 15.1R7-S6; 15.1X49 versions prior to 15.1X49-D191, 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3; 17.2 versions prior to 17.2R2-S8, 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S5; 18.2 versions prior to 18.2R2-S6, 18.2R3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R1-S5, 18.4R2; 19.1 versions prior to 19.1R1-S4, 19.1R2.</p> <p>CVE ID : CVE-2021-0244</p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-04-2021	6.8	<p>A path traversal vulnerability in the Juniper Networks SRX and vSRX Series may allow an authenticated J-web user to read sensitive system files. This issue affects Juniper Networks Junos OS on SRX and vSRX Series: 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R2-S4, 19.4R3;</p>	https://kb.juniper.net/JS_A11126	H-JUN-SRX1-040521/623

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.1 versions prior to 20.1R1-S4, 20.1R2; 20.2 versions prior to 20.2R1-S3, 20.2R2; This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1. CVE ID : CVE-2021-0231		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2021	9.3	A Cross-site Scripting (XSS) vulnerability in J-Web on Juniper Networks Junos OS allows an attacker to target another user's session thereby gaining access to the users session. The other user session must be active for the attack to succeed. Once successful, the attacker has the same privileges as the user. If the user has root privileges, the attacker may be able to gain full control of the device. This issue affects: Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S15 on EX Series; 12.3X48 versions prior to 12.3X48-D95 on SRX Series; 15.1 versions prior to 15.1R7-S6 on EX Series; 15.1X49 versions prior to 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior	https://kb.juniper.net/JS_A11166	H-JUN-SRX1-040521/624

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to 18.1R3-S9; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3; 19.1 versions prior to 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S3, 19.2R2; 19.3 versions prior to 19.3R2. CVE ID : CVE-2021-0275		
Incorrect Default Permissions	22-04-2021	4.6	On SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3, devices using tenant services on Juniper Networks Junos OS, due to incorrect default permissions assigned to tenant system administrators a tenant system administrator may inadvertently send their network traffic to one or more tenants while concurrently modifying the overall device system traffic management, affecting all tenants and the service provider. Further, a tenant may inadvertently receive traffic from another tenant. This issue affects: Juniper Networks Junos OS 18.3 version 18.3R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2; 18.3 versions prior to 18.3R3 on SRX1500, SRX4100, SRX4200, SRX4600,	https://kb.juniper.net/JS_A11139	H-JUN-SRX1-040521/625

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SRX5000 Series with SPC2; 18.4 versions prior to 18.4R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.1 versions prior to 19.1R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3. This issue does not affect: Juniper Networks Junos OS versions prior to 18.3R1. CVE ID : CVE-2021-0246		
srx210					
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-04-2021	5	An improper restriction of operations within the bounds of a memory buffer vulnerability in Juniper Networks Junos OS J-Web on SRX Series devices allows an attacker to cause Denial of Service (DoS) by sending certain crafted HTTP packets. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. When this issue occurs, web-management, NTP daemon (ntpd) and Layer 2 Control Protocol process (L2CPD) daemons might crash. This issue affects Juniper Networks Junos OS on SRX Series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4,	https://kb.juniper.net/JS_A11122	H-JUN-SRX2-040521/626

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2; CVE ID : CVE-2021-0227		
srx220					
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-04-2021	5	An improper restriction of operations within the bounds of a memory buffer vulnerability in Juniper Networks Junos OS J-Web on SRX Series devices allows an attacker to cause Denial of Service (DoS) by sending certain crafted HTTP packets. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. When this issue occurs, web-management, NTP daemon (ntpd) and Layer 2 Control Protocol process (L2CPD) daemons might crash. This issue affects Juniper Networks Junos OS on SRX Series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions	https://kb.juniper.net/JS_A11122	H-JUN-SRX2-040521/627

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2; CVE ID : CVE-2021-0227		
srx240					
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-04-2021	5	An improper restriction of operations within the bounds of a memory buffer vulnerability in Juniper Networks Junos OS J-Web on SRX Series devices allows an attacker to cause Denial of Service (DoS) by sending certain crafted HTTP packets. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. When this issue occurs, web-management, NTP daemon (ntpd) and Layer 2 Control Protocol process (L2CPD) daemons might crash. This issue affects Juniper Networks Junos OS on SRX Series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2-S1, 19.4R3; 20.1	https://kb.juniper.net/JS_A11122	H-JUN-SRX2-040521/628

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 20.1R1-S2, 20.1R2; CVE ID : CVE-2021-0227		
srx300					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-04-2021	10	On SRX Series devices configured with UTM services a buffer overflow vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS may allow an attacker to arbitrarily execute code or commands on the target to take over or otherwise impact the device by sending crafted packets to or through the device. This issue affects: Juniper Networks Junos OS on SRX Series: 15.1X49 versions prior to 15.1X49-D190; 17.4 versions prior to 17.4R2-S9; 17.4R3 and later versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S1; 18.3 versions prior to 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R2-S3, 18.4R3; 19.1 versions prior to 19.1R1-S4, 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. An indicator of compromise can be the following text in the UTM log: RT_UTM: AV_FILE_NOT_SCANNED_PASSED_MT: CVE ID : CVE-2021-0249	https://kb.juniper.net/JS_A11142	H-JUN-SRX3-040521/629
Improper Restriction of Operations within the	22-04-2021	5	An improper restriction of operations within the bounds of a memory buffer vulnerability in Juniper	https://kb.juniper.net/JS_A11122	H-JUN-SRX3-040521/630

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			<p>Networks Junos OS J-Web on SRX Series devices allows an attacker to cause Denial of Service (DoS) by sending certain crafted HTTP packets. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. When this issue occurs, web-management, NTP daemon (ntpd) and Layer 2 Control Protocol process (L2CPD) daemons might crash. This issue affects Juniper Networks Junos OS on SRX Series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2;</p> <p>CVE ID : CVE-2021-0227</p>		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	4.3	<p>A signal handler race condition exists in the Layer 2 Address Learning Daemon (L2ALD) of Juniper Networks Junos OS due to the absence of a specific protection mechanism to avoid a race condition which may allow an</p>	https://kb.juniper.net/JS_A11137	H-JUN-SRX3-040521/631

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker to bypass the storm-control feature on devices. This issue is a corner case and only occurs during specific actions taken by an administrator of a device under certain specifics actions which triggers the event. The event occurs less frequently on devices which are not configured with Virtual Chassis configurations, and more frequently on devices configured in Virtual Chassis configurations. This issue is not specific to any particular Junos OS platform. An Indicator of Compromise (IoC) may be seen by reviewing log files for the following error message seen by executing the following show statement: show log messages grep storm</p> <p>Result to look for: /kernel: GENCFG: op 58 (Storm Control Blob) failed; err 1 (Unknown) This issue affects: Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D49 on EX Series; 15.1 versions prior to 15.1R7-S6; 15.1X49 versions prior to 15.1X49-D191, 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3; 17.2 versions prior to 17.2R2-S8, 17.2R3-S3;</p>		

CVSS Scoring Scale	0-1	1-2	2-3	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-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S5; 18.2 versions prior to 18.2R2-S6, 18.2R3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R1-S5, 18.4R2; 19.1 versions prior to 19.1R1-S4, 19.1R2. CVE ID : CVE-2021-0244								
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-04-2021	6.8	A path traversal vulnerability in the Juniper Networks SRX and vSRX Series may allow an authenticated J-web user to read sensitive system files. This issue affects Juniper Networks Junos OS on SRX and vSRX Series: 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R2-S4, 19.4R3; 20.1 versions prior to 20.1R1-S4, 20.1R2; 20.2 versions prior to 20.2R1-S3, 20.2R2; This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1. CVE ID : CVE-2021-0231	https://kb.juniper.net/JS_A11126	H-JUN-SRX3-040521/632						
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2021	9.3	A Cross-site Scripting (XSS) vulnerability in J-Web on Juniper Networks Junos OS allows an attacker to target another user's session thereby gaining access to the users session. The other user session must be active for the attack to succeed. Once successful, the	https://kb.juniper.net/JS_A11166	H-JUN-SRX3-040521/633						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker has the same privileges as the user. If the user has root privileges, the attacker may be able to gain full control of the device.</p> <p>This issue affects: Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S15 on EX Series; 12.3X48 versions prior to 12.3X48-D95 on SRX Series; 15.1 versions prior to 15.1R7-S6 on EX Series; 15.1X49 versions prior to 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3; 19.1 versions prior to 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S3, 19.2R2; 19.3 versions prior to 19.3R2.</p> <p>CVE ID : CVE-2021-0275</p>		
srx320					
Buffer Copy without Checking Size of Input ('Classic	22-04-2021	10	On SRX Series devices configured with UTM services a buffer overflow vulnerability in the Packet Forwarding Engine (PFE) of	https://kb.juniper.net/JS_A11142	H-JUN-SRX3-040521/634

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			<p>Juniper Networks Junos OS may allow an attacker to arbitrarily execute code or commands on the target to take over or otherwise impact the device by sending crafted packets to or through the device. This issue affects: Juniper Networks Junos OS on SRX Series: 15.1X49 versions prior to 15.1X49-D190; 17.4 versions prior to 17.4R2-S9; 17.4R3 and later versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S1; 18.3 versions prior to 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R2-S3, 18.4R3; 19.1 versions prior to 19.1R1-S4, 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. An indicator of compromise can be the following text in the UTM log: RT_UTM: AV_FILE_NOT_SCANNED_PASSED_MT:</p> <p>CVE ID : CVE-2021-0249</p>		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-04-2021	5	<p>An improper restriction of operations within the bounds of a memory buffer vulnerability in Juniper Networks Junos OS J-Web on SRX Series devices allows an attacker to cause Denial of Service (DoS) by sending certain crafted HTTP packets. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. When this</p>	https://kb.juniper.net/JS_A11122	H-JUN-SRX3-040521/635

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>issue occurs, web-management, NTP daemon (ntpd) and Layer 2 Control Protocol process (L2CPD) daemons might crash. This issue affects Juniper Networks Junos OS on SRX Series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2;</p> <p>CVE ID : CVE-2021-0227</p>		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	4.3	<p>A signal handler race condition exists in the Layer 2 Address Learning Daemon (L2ALD) of Juniper Networks Junos OS due to the absence of a specific protection mechanism to avoid a race condition which may allow an attacker to bypass the storm-control feature on devices. This issue is a corner case and only occurs during specific actions taken by an administrator of a device under certain specific actions which triggers the event. The event occurs less frequently</p>	https://kb.juniper.net/JS_A11137	H-JUN-SRX3-040521/636

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>on devices which are not configured with Virtual Chassis configurations, and more frequently on devices configured in Virtual Chassis configurations. This issue is not specific to any particular Junos OS platform. An Indicator of Compromise (IoC) may be seen by reviewing log files for the following error message seen by executing the following show statement: show log messages grep storm</p> <p>Result to look for: /kernel: GENCFG: op 58 (Storm Control Blob) failed; err 1 (Unknown) This issue affects: Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D49 on EX Series; 15.1 versions prior to 15.1R7-S6; 15.1X49 versions prior to 15.1X49-D191, 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3; 17.2 versions prior to 17.2R2-S8, 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S5; 18.2 versions prior to 18.2R2-S6, 18.2R3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R1-S5, 18.4R2; 19.1</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			versions prior to 19.1R1-S4, 19.1R2. CVE ID : CVE-2021-0244								
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-04-2021	6.8	A path traversal vulnerability in the Juniper Networks SRX and vSRX Series may allow an authenticated J-web user to read sensitive system files. This issue affects Juniper Networks Junos OS on SRX and vSRX Series: 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R2-S4, 19.4R3; 20.1 versions prior to 20.1R1-S4, 20.1R2; 20.2 versions prior to 20.2R1-S3, 20.2R2; This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1. CVE ID : CVE-2021-0231	https://kb.juniper.net/JS_A11126	H-JUN-SRX3-040521/637						
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2021	9.3	A Cross-site Scripting (XSS) vulnerability in J-Web on Juniper Networks Junos OS allows an attacker to target another user's session thereby gaining access to the users session. The other user session must be active for the attack to succeed. Once successful, the attacker has the same privileges as the user. If the user has root privileges, the attacker may be able to gain full control of the device. This issue affects: Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S15 on EX Series; 12.3X48 versions prior to 12.3X48-	https://kb.juniper.net/JS_A11166	H-JUN-SRX3-040521/638						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>D95 on SRX Series; 15.1 versions prior to 15.1R7-S6 on EX Series; 15.1X49 versions prior to 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3; 19.1 versions prior to 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S3, 19.2R2; 19.3 versions prior to 19.3R2.</p> <p>CVE ID : CVE-2021-0275</p>		
srx340					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-04-2021	10	<p>On SRX Series devices configured with UTM services a buffer overflow vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS may allow an attacker to arbitrarily execute code or commands on the target to take over or otherwise impact the device by sending crafted packets to or through the device. This issue affects: Juniper Networks Junos OS on SRX</p>	https://kb.juniper.net/JS_A11142	H-JUN-SRX3-040521/639

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series: 15.1X49 versions prior to 15.1X49-D190; 17.4 versions prior to 17.4R2-S9; 17.4R3 and later versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S1; 18.3 versions prior to 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R2-S3, 18.4R3; 19.1 versions prior to 19.1R1-S4, 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. An indicator of compromise can be the following text in the UTM log: RT_UTM: AV_FILE_NOT_SCANNED_PASSED_MT: CVE ID : CVE-2021-0249		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-04-2021	5	An improper restriction of operations within the bounds of a memory buffer vulnerability in Juniper Networks Junos OS J-Web on SRX Series devices allows an attacker to cause Denial of Service (DoS) by sending certain crafted HTTP packets. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. When this issue occurs, web-management, NTP daemon (ntpd) and Layer 2 Control Protocol process (L2CPD) daemons might crash. This issue affects Juniper Networks Junos OS on SRX Series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11,	https://kb.juniper.net/JS_A11122	H-JUN-SRX3-040521/640

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			17.4R3-S2; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2; CVE ID : CVE-2021-0227		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	4.3	A signal handler race condition exists in the Layer 2 Address Learning Daemon (L2ALD) of Juniper Networks Junos OS due to the absence of a specific protection mechanism to avoid a race condition which may allow an attacker to bypass the storm-control feature on devices. This issue is a corner case and only occurs during specific actions taken by an administrator of a device under certain specific actions which triggers the event. The event occurs less frequently on devices which are not configured with Virtual Chassis configurations, and more frequently on devices configured in Virtual Chassis configurations. This issue is not specific to any particular Junos OS platform. An Indicator of Compromise (IoC) may be	https://kb.juniper.net/JS_A11137	H-JUN-SRX3-040521/641

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>seen by reviewing log files for the following error message seen by executing the following show statement: show log messages grep storm Result to look for: /kernel: GENCFG: op 58 (Storm Control Blob) failed; err 1 (Unknown) This issue affects: Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D49 on EX Series; 15.1 versions prior to 15.1R7-S6; 15.1X49 versions prior to 15.1X49-D191, 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3; 17.2 versions prior to 17.2R2-S8, 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S5; 18.2 versions prior to 18.2R2-S6, 18.2R3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R1-S5, 18.4R2; 19.1 versions prior to 19.1R1-S4, 19.1R2.</p> <p>CVE ID : CVE-2021-0244</p>		
Improper Limitation of a Pathname to a Restricted Directory	22-04-2021	6.8	<p>A path traversal vulnerability in the Juniper Networks SRX and vSRX Series may allow an authenticated J-web user to read sensitive system files.</p>	https://kb.juniper.net/JS_A11126	H-JUN-SRX3-040521/642

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			This issue affects Juniper Networks Junos OS on SRX and vSRX Series: 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R2-S4, 19.4R3; 20.1 versions prior to 20.1R1-S4, 20.1R2; 20.2 versions prior to 20.2R1-S3, 20.2R2; This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1. CVE ID : CVE-2021-0231		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2021	9.3	A Cross-site Scripting (XSS) vulnerability in J-Web on Juniper Networks Junos OS allows an attacker to target another user's session thereby gaining access to the users session. The other user session must be active for the attack to succeed. Once successful, the attacker has the same privileges as the user. If the user has root privileges, the attacker may be able to gain full control of the device. This issue affects: Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S15 on EX Series; 12.3X48 versions prior to 12.3X48-D95 on SRX Series; 15.1 versions prior to 15.1R7-S6 on EX Series; 15.1X49 versions prior to 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-	https://kb.juniper.net/JS_A11166	H-JUN-SRX3-040521/643

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S11, 17.1R3-S2; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3; 19.1 versions prior to 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S3, 19.2R2; 19.3 versions prior to 19.3R2. CVE ID : CVE-2021-0275		

srx3400

Improper Restriction of Operations within the Bounds of a Memory Buffer	22-04-2021	5	An improper restriction of operations within the bounds of a memory buffer vulnerability in Juniper Networks Junos OS J-Web on SRX Series devices allows an attacker to cause Denial of Service (DoS) by sending certain crafted HTTP packets. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. When this issue occurs, web-management, NTP daemon (ntpd) and Layer 2 Control Protocol process (L2CPD) daemons might crash. This issue affects Juniper Networks Junos OS on SRX Series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11,	https://kb.juniper.net/JS_A11122	H-JUN-SRX3-040521/644
---	------------	---	--	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			17.4R3-S2; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2; CVE ID : CVE-2021-0227		

srx345

Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-04-2021	10	On SRX Series devices configured with UTM services a buffer overflow vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS may allow an attacker to arbitrarily execute code or commands on the target to take over or otherwise impact the device by sending crafted packets to or through the device. This issue affects: Juniper Networks Junos OS on SRX Series: 15.1X49 versions prior to 15.1X49-D190; 17.4 versions prior to 17.4R2-S9; 17.4R3 and later versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S1; 18.3 versions prior to 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R2-S3, 18.4R3; 19.1 versions prior to 19.1R1-S4, 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. An indicator of	https://kb.juniper.net/JS_A11142	H-JUN-SRX3-040521/645
--	------------	----	---	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			compromise can be the following text in the UTM log: RT_UTM: AV_FILE_NOT_SCANNED_PASSED_MT: CVE ID : CVE-2021-0249		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-04-2021	5	An improper restriction of operations within the bounds of a memory buffer vulnerability in Juniper Networks Junos OS J-Web on SRX Series devices allows an attacker to cause Denial of Service (DoS) by sending certain crafted HTTP packets. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. When this issue occurs, web-management, NTP daemon (ntpd) and Layer 2 Control Protocol process (L2CPD) daemons might crash. This issue affects Juniper Networks Junos OS on SRX Series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2;	https://kb.juniper.net/JS_A11122	H-JUN-SRX3-040521/646

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-0227							
Concurrent Execution using Shared Resource with Improper Synchronizati on ('Race Condition')	22-04-2021	4.3	A signal handler race condition exists in the Layer 2 Address Learning Daemon (L2ALD) of Juniper Networks Junos OS due to the absence of a specific protection mechanism to avoid a race condition which may allow an attacker to bypass the storm-control feature on devices. This issue is a corner case and only occurs during specific actions taken by an administrator of a device under certain specifics actions which triggers the event. The event occurs less frequently on devices which are not configured with Virtual Chassis configurations, and more frequently on devices configured in Virtual Chassis configurations. This issue is not specific to any particular Junos OS platform. An Indicator of Compromise (IoC) may be seen by reviewing log files for the following error message seen by executing the following show statement: show log messages grep storm Result to look for: /kernel: GENCFG: op 58 (Storm Control Blob) failed; err 1 (Unknown) This issue affects: Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D49 on EX Series; 15.1 versions prior	https://kb.juniper.net/JS_A11137	H-JUN-SRX3-040521/647					
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
			to 15.1R7-S6; 15.1X49 versions prior to 15.1X49-D191, 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3; 17.2 versions prior to 17.2R2-S8, 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S5; 18.2 versions prior to 18.2R2-S6, 18.2R3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R1-S5, 18.4R2; 19.1 versions prior to 19.1R1-S4, 19.1R2. CVE ID : CVE-2021-0244		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-04-2021	6.8	A path traversal vulnerability in the Juniper Networks SRX and vSRX Series may allow an authenticated J-web user to read sensitive system files. This issue affects Juniper Networks Junos OS on SRX and vSRX Series: 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R2-S4, 19.4R3; 20.1 versions prior to 20.1R1-S4, 20.1R2; 20.2 versions prior to 20.2R1-S3, 20.2R2; This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1. CVE ID : CVE-2021-0231	https://kb.juniper.net/JS_A11126	H-JUN-SRX3-040521/648

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2021	9.3	A Cross-site Scripting (XSS) vulnerability in J-Web on Juniper Networks Junos OS allows an attacker to target another user's session thereby gaining access to the users session. The other user session must be active for the attack to succeed. Once successful, the attacker has the same privileges as the user. If the user has root privileges, the attacker may be able to gain full control of the device. This issue affects: Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S15 on EX Series; 12.3X48 versions prior to 12.3X48-D95 on SRX Series; 15.1 versions prior to 15.1R7-S6 on EX Series; 15.1X49 versions prior to 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3; 19.1 versions prior to 19.1R2-S1, 19.1R3; 19.2 versions prior to	https://kb.juniper.net/JS_A11166	H-JUN-SRX3-040521/649

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.2R1-S3, 19.2R2; 19.3 versions prior to 19.3R2. CVE ID : CVE-2021-0275		
srx3600					
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-04-2021	5	An improper restriction of operations within the bounds of a memory buffer vulnerability in Juniper Networks Junos OS J-Web on SRX Series devices allows an attacker to cause Denial of Service (DoS) by sending certain crafted HTTP packets. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. When this issue occurs, web-management, NTP daemon (ntpd) and Layer 2 Control Protocol process (L2CPD) daemons might crash. This issue affects Juniper Networks Junos OS on SRX Series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2; CVE ID : CVE-2021-0227	https://kb.juniper.net/JS_A11122	H-JUN-SRX3-040521/650

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
srx380					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-04-2021	10	On SRX Series devices configured with UTM services a buffer overflow vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS may allow an attacker to arbitrarily execute code or commands on the target to take over or otherwise impact the device by sending crafted packets to or through the device. This issue affects: Juniper Networks Junos OS on SRX Series: 15.1X49 versions prior to 15.1X49-D190; 17.4 versions prior to 17.4R2-S9; 17.4R3 and later versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S1; 18.3 versions prior to 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R2-S3, 18.4R3; 19.1 versions prior to 19.1R1-S4, 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. An indicator of compromise can be the following text in the UTM log: RT_UTM: AV_FILE_NOT_SCANNED_PASSED_MT: CVE ID : CVE-2021-0249	https://kb.juniper.net/JS_A11142	H-JUN-SRX3-040521/651
Concurrent Execution using Shared Resource with Improper Synchronization ('Race')	22-04-2021	4.3	A signal handler race condition exists in the Layer 2 Address Learning Daemon (L2ALD) of Juniper Networks Junos OS due to the absence of a specific protection mechanism to avoid a race condition	https://kb.juniper.net/JS_A11137	H-JUN-SRX3-040521/652

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Condition')			<p>which may allow an attacker to bypass the storm-control feature on devices. This issue is a corner case and only occurs during specific actions taken by an administrator of a device under certain specifics actions which triggers the event. The event occurs less frequently on devices which are not configured with Virtual Chassis configurations, and more frequently on devices configured in Virtual Chassis configurations. This issue is not specific to any particular Junos OS platform. An Indicator of Compromise (IoC) may be seen by reviewing log files for the following error message seen by executing the following show statement: show log messages grep storm</p> <p>Result to look for: /kernel: GENCFG: op 58 (Storm Control Blob) failed; err 1 (Unknown) This issue affects: Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D49 on EX Series; 15.1 versions prior to 15.1R7-S6; 15.1X49 versions prior to 15.1X49-D191, 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3; 17.2 versions prior</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			to 17.2R2-S8, 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S5; 18.2 versions prior to 18.2R2-S6, 18.2R3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R1-S5, 18.4R2; 19.1 versions prior to 19.1R1-S4, 19.1R2. CVE ID : CVE-2021-0244								
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-04-2021	6.8	A path traversal vulnerability in the Juniper Networks SRX and vSRX Series may allow an authenticated J-web user to read sensitive system files. This issue affects Juniper Networks Junos OS on SRX and vSRX Series: 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R2-S4, 19.4R3; 20.1 versions prior to 20.1R1-S4, 20.1R2; 20.2 versions prior to 20.2R1-S3, 20.2R2; This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1. CVE ID : CVE-2021-0231	https://kb.juniper.net/JS_A11126	H-JUN-SRX3-040521/653						
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2021	9.3	A Cross-site Scripting (XSS) vulnerability in J-Web on Juniper Networks Junos OS allows an attacker to target another user's session thereby gaining access to the users session. The other user session must be active for the attack to succeed.	https://kb.juniper.net/JS_A11166	H-JUN-SRX3-040521/654						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Once successful, the attacker has the same privileges as the user. If the user has root privileges, the attacker may be able to gain full control of the device.</p> <p>This issue affects: Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S15 on EX Series; 12.3X48 versions prior to 12.3X48-D95 on SRX Series; 15.1 versions prior to 15.1R7-S6 on EX Series; 15.1X49 versions prior to 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3; 19.1 versions prior to 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S3, 19.2R2; 19.3 versions prior to 19.3R2.</p> <p>CVE ID : CVE-2021-0275</p>		
srx4100					
Incorrect Default Permissions	22-04-2021	4.6	On SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3, vSRX Series	https://kb.juniper.net/JS_A11130	H-JUN-SRX4-040521/655

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>devices using tenant services on Juniper Networks Junos OS, due to incorrect permission scheme assigned to tenant system administrators, a tenant system administrator may inadvertently send their network traffic to one or more tenants while concurrently modifying the overall device system traffic management, affecting all tenants and the service provider. Further, a tenant may inadvertently receive traffic from another tenant. This issue affects: Juniper Networks Junos OS 18.3 version 18.3R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2; 18.4 version 18.4R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.1 versions 19.1R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.3 versions prior to 19.3R3-S2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SPC2/SPC3; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 20.1 versions prior to 20.1R2, 20.1R3 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series; 20.2 versions prior to 20.2R2-S1, 20.2R3 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series; 20.3 versions prior to 20.3R1-S2, 20.3R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series; 20.4 versions prior to 20.4R1, 20.4R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 18.3R1. CVE ID : CVE-2021-0235		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-04-2021	10	On SRX Series devices configured with UTM services a buffer overflow vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS may allow an attacker to arbitrarily execute code or commands on the target to take over or otherwise	https://kb.juniper.net/JS_A11142	H-JUN-SRX4-040521/656

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>impact the device by sending crafted packets to or through the device. This issue affects: Juniper Networks Junos OS on SRX Series: 15.1X49 versions prior to 15.1X49-D190; 17.4 versions prior to 17.4R2-S9; 17.4R3 and later versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S1; 18.3 versions prior to 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R2-S3, 18.4R3; 19.1 versions prior to 19.1R1-S4, 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. An indicator of compromise can be the following text in the UTM log: RT_UTM: AV_FILE_NOT_SCANNED_PASSED_MT:</p> <p>CVE ID : CVE-2021-0249</p>		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-04-2021	5	<p>An improper restriction of operations within the bounds of a memory buffer vulnerability in Juniper Networks Junos OS J-Web on SRX Series devices allows an attacker to cause Denial of Service (DoS) by sending certain crafted HTTP packets. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. When this issue occurs, web-management, NTP daemon (ntpd) and Layer 2 Control Protocol process (L2CPD) daemons might crash. This</p>	https://kb.juniper.net/JS_A11122	H-JUN-SRX4-040521/657

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>issue affects Juniper Networks Junos OS on SRX Series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2;</p> <p>CVE ID : CVE-2021-0227</p>		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	4.3	<p>A signal handler race condition exists in the Layer 2 Address Learning Daemon (L2ALD) of Juniper Networks Junos OS due to the absence of a specific protection mechanism to avoid a race condition which may allow an attacker to bypass the storm-control feature on devices. This issue is a corner case and only occurs during specific actions taken by an administrator of a device under certain specific actions which triggers the event. The event occurs less frequently on devices which are not configured with Virtual Chassis configurations, and more frequently on devices configured in Virtual</p>	https://kb.juniper.net/JS_A11137	H-JUN-SRX4-040521/658

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Chassis configurations. This issue is not specific to any particular Junos OS platform. An Indicator of Compromise (IoC) may be seen by reviewing log files for the following error message seen by executing the following show statement: show log messages grep storm</p> <p>Result to look for: /kernel: GENCFG: op 58 (Storm Control Blob) failed; err 1 (Unknown) This issue affects: Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D49 on EX Series; 15.1 versions prior to 15.1R7-S6; 15.1X49 versions prior to 15.1X49-D191, 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3; 17.2 versions prior to 17.2R2-S8, 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S5; 18.2 versions prior to 18.2R2-S6, 18.2R3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R1-S5, 18.4R2; 19.1 versions prior to 19.1R1-S4, 19.1R2.</p> <p>CVE ID : CVE-2021-0244</p>		
Improper	22-04-2021	6.8	A path traversal	https://kb.ju	H-JUN-SRX4-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Limitation of a Pathname to a Restricted Directory ('Path Traversal')			vulnerability in the Juniper Networks SRX and vSRX Series may allow an authenticated J-web user to read sensitive system files. This issue affects Juniper Networks Junos OS on SRX and vSRX Series: 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R2-S4, 19.4R3; 20.1 versions prior to 20.1R1-S4, 20.1R2; 20.2 versions prior to 20.2R1-S3, 20.2R2; This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1. CVE ID : CVE-2021-0231	niper.net/JS A11126	040521/659
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2021	9.3	A Cross-site Scripting (XSS) vulnerability in J-Web on Juniper Networks Junos OS allows an attacker to target another user's session thereby gaining access to the users session. The other user session must be active for the attack to succeed. Once successful, the attacker has the same privileges as the user. If the user has root privileges, the attacker may be able to gain full control of the device. This issue affects: Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S15 on EX Series; 12.3X48 versions prior to 12.3X48-D95 on SRX Series; 15.1 versions prior to 15.1R7-S6 on EX Series; 15.1X49 versions prior to 15.1X49-	https://kb.juniper.net/JS A11166	H-JUN-SRX4-040521/660

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3; 19.1 versions prior to 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S3, 19.2R2; 19.3 versions prior to 19.3R2. CVE ID : CVE-2021-0275		
Incorrect Default Permissions	22-04-2021	4.6	On SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3, devices using tenant services on Juniper Networks Junos OS, due to incorrect default permissions assigned to tenant system administrators a tenant system administrator may inadvertently send their network traffic to one or more tenants while concurrently modifying the overall device system traffic management, affecting all tenants and the service provider. Further, a tenant may inadvertently receive	https://kb.juniper.net/JS_A11139	H-JUN-SRX4-040521/661

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>traffic from another tenant. This issue affects: Juniper Networks Junos OS 18.3 version 18.3R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2; 18.3 versions prior to 18.3R3 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2; 18.4 versions prior to 18.4R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.1 versions prior to 19.1R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3. This issue does not affect: Juniper Networks Junos OS versions prior to 18.3R1.</p> <p>CVE ID : CVE-2021-0246</p>		
srx4200					
Incorrect Default Permissions	22-04-2021	4.6	<p>On SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3, vSRX Series devices using tenant services on Juniper Networks Junos OS, due to incorrect permission scheme assigned to tenant system administrators, a tenant system administrator may inadvertently send their network traffic to one or more tenants while concurrently modifying the</p>	https://kb.juniper.net/JS_A11130	H-JUN-SRX4-040521/662

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>overall device system traffic management, affecting all tenants and the service provider. Further, a tenant may inadvertently receive traffic from another tenant. This issue affects: Juniper Networks Junos OS 18.3 version 18.3R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2; 18.4 version 18.4R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.1 versions 19.1R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.3 versions prior to 19.3R3-S2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 20.1 versions prior to 20.1R2, 20.1R3 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series; 20.2 versions prior to</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>20.2R2-S1, 20.2R3 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series; 20.3 versions prior to 20.3R1-S2, 20.3R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series; 20.4 versions prior to 20.4R1, 20.4R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series.</p> <p>This issue does not affect Juniper Networks Junos OS versions prior to 18.3R1.</p> <p>CVE ID : CVE-2021-0235</p>		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-04-2021	10	<p>On SRX Series devices configured with UTM services a buffer overflow vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS may allow an attacker to arbitrarily execute code or commands on the target to take over or otherwise impact the device by sending crafted packets to or through the device. This issue affects: Juniper Networks Junos OS on SRX Series: 15.1X49 versions prior to 15.1X49-D190; 17.4 versions prior to 17.4R2-S9; 17.4R3 and later versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S1; 18.3 versions prior to</p>	https://kb.juniper.net/JS_A11142	H-JUN-SRX4-040521/663

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R2-S3, 18.4R3; 19.1 versions prior to 19.1R1-S4, 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. An indicator of compromise can be the following text in the UTM log: RT_UTM: AV_FILE_NOT_SCANNED_PASSED_MT: CVE ID : CVE-2021-0249		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-04-2021	5	An improper restriction of operations within the bounds of a memory buffer vulnerability in Juniper Networks Junos OS J-Web on SRX Series devices allows an attacker to cause Denial of Service (DoS) by sending certain crafted HTTP packets. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. When this issue occurs, web-management, NTP daemon (ntpd) and Layer 2 Control Protocol process (L2CPD) daemons might crash. This issue affects Juniper Networks Junos OS on SRX Series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions	https://kb.juniper.net/JS_A11122	H-JUN-SRX4-040521/664

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2; CVE ID : CVE-2021-0227		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	4.3	A signal handler race condition exists in the Layer 2 Address Learning Daemon (L2ALD) of Juniper Networks Junos OS due to the absence of a specific protection mechanism to avoid a race condition which may allow an attacker to bypass the storm-control feature on devices. This issue is a corner case and only occurs during specific actions taken by an administrator of a device under certain specific actions which triggers the event. The event occurs less frequently on devices which are not configured with Virtual Chassis configurations, and more frequently on devices configured in Virtual Chassis configurations. This issue is not specific to any particular Junos OS platform. An Indicator of Compromise (IoC) may be seen by reviewing log files for the following error message seen by executing the following show statement: show log messages grep storm Result to look for: /kernel:	https://kb.juniper.net/JS_A11137	H-JUN-SRX4-040521/665

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>GENCFG: op 58 (Storm Control Blob) failed; err 1 (Unknown) This issue affects: Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D49 on EX Series; 15.1 versions prior to 15.1R7-S6; 15.1X49 versions prior to 15.1X49-D191, 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3; 17.2 versions prior to 17.2R2-S8, 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S5; 18.2 versions prior to 18.2R2-S6, 18.2R3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R1-S5, 18.4R2; 19.1 versions prior to 19.1R1-S4, 19.1R2.</p> <p>CVE ID : CVE-2021-0244</p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-04-2021	6.8	<p>A path traversal vulnerability in the Juniper Networks SRX and vSRX Series may allow an authenticated J-web user to read sensitive system files. This issue affects Juniper Networks Junos OS on SRX and vSRX Series: 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R2-S4, 19.4R3; 20.1 versions prior to</p>	https://kb.juniper.net/JS_A11126	H-JUN-SRX4-040521/666

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.1R1-S4, 20.1R2; 20.2 versions prior to 20.2R1-S3, 20.2R2; This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1. CVE ID : CVE-2021-0231		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2021	9.3	A Cross-site Scripting (XSS) vulnerability in J-Web on Juniper Networks Junos OS allows an attacker to target another user's session thereby gaining access to the users session. The other user session must be active for the attack to succeed. Once successful, the attacker has the same privileges as the user. If the user has root privileges, the attacker may be able to gain full control of the device. This issue affects: Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S15 on EX Series; 12.3X48 versions prior to 12.3X48-D95 on SRX Series; 15.1 versions prior to 15.1R7-S6 on EX Series; 15.1X49 versions prior to 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S9; 18.2 versions	https://kb.juniper.net/JS_A11166	H-JUN-SRX4-040521/667

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3; 19.1 versions prior to 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S3, 19.2R2; 19.3 versions prior to 19.3R2.</p> <p>CVE ID : CVE-2021-0275</p>		
Incorrect Default Permissions	22-04-2021	4.6	<p>On SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3, devices using tenant services on Juniper Networks Junos OS, due to incorrect default permissions assigned to tenant system administrators a tenant system administrator may inadvertently send their network traffic to one or more tenants while concurrently modifying the overall device system traffic management, affecting all tenants and the service provider. Further, a tenant may inadvertently receive traffic from another tenant. This issue affects: Juniper Networks Junos OS 18.3 version 18.3R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2; 18.3 versions prior to 18.3R3 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2;</p>	https://kb.juniper.net/JS_A11139	H-JUN-SRX4-040521/668

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.4 versions prior to 18.4R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.1 versions prior to 19.1R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3. This issue does not affect: Juniper Networks Junos OS versions prior to 18.3R1. CVE ID : CVE-2021-0246		
srx4600					
Incorrect Default Permissions	22-04-2021	4.6	On SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3, vSRX Series devices using tenant services on Juniper Networks Junos OS, due to incorrect permission scheme assigned to tenant system administrators, a tenant system administrator may inadvertently send their network traffic to one or more tenants while concurrently modifying the overall device system traffic management, affecting all tenants and the service provider. Further, a tenant may inadvertently receive traffic from another tenant. This issue affects: Juniper Networks Junos OS 18.3 version 18.3R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series	https://kb.juniper.net/JS_A11130	H-JUN-SRX4-040521/669

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>with SPC2; 18.4 version 18.4R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.1 versions 19.1R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.3 versions prior to 19.3R3-S2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series; 20.1 versions prior to 20.1R2, 20.1R3 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series; 20.2 versions prior to 20.2R2-S1, 20.2R3 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series; 20.3 versions prior to 20.3R1-S2, 20.3R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series; 20.4 versions prior to</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.4R1, 20.4R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 18.3R1. CVE ID : CVE-2021-0235		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-04-2021	10	On SRX Series devices configured with UTM services a buffer overflow vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS may allow an attacker to arbitrarily execute code or commands on the target to take over or otherwise impact the device by sending crafted packets to or through the device. This issue affects: Juniper Networks Junos OS on SRX Series: 15.1X49 versions prior to 15.1X49-D190; 17.4 versions prior to 17.4R2-S9; 17.4R3 and later versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S1; 18.3 versions prior to 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R2-S3, 18.4R3; 19.1 versions prior to 19.1R1-S4, 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. An indicator of compromise can be the following text in the UTM log: RT_UTM: AV_FILE_NOT_SCANNED_PASSED_MT: CVE ID : CVE-2021-0249	https://kb.juniper.net/JS_A11142	H-JUN-SRX4-040521/670

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-04-2021	5	<p>An improper restriction of operations within the bounds of a memory buffer vulnerability in Juniper Networks Junos OS J-Web on SRX Series devices allows an attacker to cause Denial of Service (DoS) by sending certain crafted HTTP packets. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. When this issue occurs, web-management, NTP daemon (ntpd) and Layer 2 Control Protocol process (L2CPD) daemons might crash. This issue affects Juniper Networks Junos OS on SRX Series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2;</p> <p>CVE ID : CVE-2021-0227</p>	https://kb.juniper.net/JS_A11122	H-JUN-SRX4-040521/671
Concurrent Execution using Shared Resource with	22-04-2021	4.3	<p>A signal handler race condition exists in the Layer 2 Address Learning Daemon (L2ALD) of Juniper Networks Junos OS due to</p>	https://kb.juniper.net/JS_A11137	H-JUN-SRX4-040521/672

CVSS Scoring Scale	0-1	1-2	2-3	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 Synchronization ('Race Condition')			the absence of a specific protection mechanism to avoid a race condition which may allow an attacker to bypass the storm-control feature on devices. This issue is a corner case and only occurs during specific actions taken by an administrator of a device under certain specific actions which triggers the event. The event occurs less frequently on devices which are not configured with Virtual Chassis configurations, and more frequently on devices configured in Virtual Chassis configurations. This issue is not specific to any particular Junos OS platform. An Indicator of Compromise (IoC) may be seen by reviewing log files for the following error message seen by executing the following show statement: show log messages grep storm Result to look for: /kernel: GENCFG: op 58 (Storm Control Blob) failed; err 1 (Unknown) This issue affects: Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D49 on EX Series; 15.1 versions prior to 15.1R7-S6; 15.1X49 versions prior to 15.1X49-D191, 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-		

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						
			S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3; 17.2 versions prior to 17.2R2-S8, 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S5; 18.2 versions prior to 18.2R2-S6, 18.2R3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R1-S5, 18.4R2; 19.1 versions prior to 19.1R1-S4, 19.1R2. CVE ID : CVE-2021-0244								
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-04-2021	6.8	A path traversal vulnerability in the Juniper Networks SRX and vSRX Series may allow an authenticated J-web user to read sensitive system files. This issue affects Juniper Networks Junos OS on SRX and vSRX Series: 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R2-S4, 19.4R3; 20.1 versions prior to 20.1R1-S4, 20.1R2; 20.2 versions prior to 20.2R1-S3, 20.2R2; This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1. CVE ID : CVE-2021-0231	https://kb.juniper.net/JS_A11126	H-JUN-SRX4-040521/673						
Improper Neutralization of Input During Web Page Generation	22-04-2021	9.3	A Cross-site Scripting (XSS) vulnerability in J-Web on Juniper Networks Junos OS allows an attacker to target another user's session thereby gaining access to	https://kb.juniper.net/JS_A11166	H-JUN-SRX4-040521/674						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			<p>the users session. The other user session must be active for the attack to succeed. Once successful, the attacker has the same privileges as the user. If the user has root privileges, the attacker may be able to gain full control of the device. This issue affects: Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S15 on EX Series; 12.3X48 versions prior to 12.3X48-D95 on SRX Series; 15.1 versions prior to 15.1R7-S6 on EX Series; 15.1X49 versions prior to 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3; 19.1 versions prior to 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S3, 19.2R2; 19.3 versions prior to 19.3R2.</p> <p>CVE ID : CVE-2021-0275</p>		
Incorrect Default	22-04-2021	4.6	On SRX1500, SRX4100, SRX4200, SRX4600,	https://kb.juniper.net/JS	H-JUN-SRX4-040521/675

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Permissions			<p>SRX5000 Series with SPC2/SPC3, devices using tenant services on Juniper Networks Junos OS, due to incorrect default permissions assigned to tenant system administrators a tenant system administrator may inadvertently send their network traffic to one or more tenants while concurrently modifying the overall device system traffic management, affecting all tenants and the service provider. Further, a tenant may inadvertently receive traffic from another tenant. This issue affects: Juniper Networks Junos OS 18.3 version 18.3R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2; 18.3 versions prior to 18.3R3 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2; 18.4 versions prior to 18.4R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.1 versions prior to 19.1R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3. This issue does not affect: Juniper Networks Junos OS versions prior to 18.3R1.</p>	A11139	

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-0246		
srx5000					
Incorrect Default Permissions	22-04-2021	4.6	On SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3, vSRX Series devices using tenant services on Juniper Networks Junos OS, due to incorrect permission scheme assigned to tenant system administrators, a tenant system administrator may inadvertently send their network traffic to one or more tenants while concurrently modifying the overall device system traffic management, affecting all tenants and the service provider. Further, a tenant may inadvertently receive traffic from another tenant. This issue affects: Juniper Networks Junos OS 18.3 version 18.3R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2; 18.4 version 18.4R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.1 versions 19.1R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2 on SRX1500, SRX4100,	https://kb.juniper.net/JS_A11130	H-JUN-SRX5-040521/676

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.3 versions prior to 19.3R3-S2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 20.1 versions prior to 20.1R2, 20.1R3 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series; 20.2 versions prior to 20.2R2-S1, 20.2R3 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series; 20.3 versions prior to 20.3R1-S2, 20.3R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series; 20.4 versions prior to 20.4R1, 20.4R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 18.3R1. CVE ID : CVE-2021-0235							
srx5400										
Buffer Copy without	22-04-2021	10	On SRX Series devices configured with UTM	https://kb.juniper.net/JS	H-JUN-SRX5-040521/677					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			services a buffer overflow vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS may allow an attacker to arbitrarily execute code or commands on the target to take over or otherwise impact the device by sending crafted packets to or through the device. This issue affects: Juniper Networks Junos OS on SRX Series: 15.1X49 versions prior to 15.1X49-D190; 17.4 versions prior to 17.4R2-S9; 17.4R3 and later versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S1; 18.3 versions prior to 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R2-S3, 18.4R3; 19.1 versions prior to 19.1R1-S4, 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. An indicator of compromise can be the following text in the UTM log: RT_UTM: AV_FILE_NOT_SCANNED_PASSED_MT: CVE ID : CVE-2021-0249	A11142	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-04-2021	5	An improper restriction of operations within the bounds of a memory buffer vulnerability in Juniper Networks Junos OS J-Web on SRX Series devices allows an attacker to cause Denial of Service (DoS) by sending certain crafted HTTP packets. Continued receipt and processing of	https://kb.juniper.net/JS_A11122	H-JUN-SRX5-040521/678

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			these packets will create a sustained Denial of Service (DoS) condition. When this issue occurs, web-management, NTP daemon (ntpd) and Layer 2 Control Protocol process (L2CPD) daemons might crash. This issue affects Juniper Networks Junos OS on SRX Series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2; CVE ID : CVE-2021-0227		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	4.3	A signal handler race condition exists in the Layer 2 Address Learning Daemon (L2ALD) of Juniper Networks Junos OS due to the absence of a specific protection mechanism to avoid a race condition which may allow an attacker to bypass the storm-control feature on devices. This issue is a corner case and only occurs during specific actions taken by an administrator of a device under certain	https://kb.juniper.net/JS_A11137	H-JUN-SRX5-040521/679

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>specifics actions which triggers the event. The event occurs less frequently on devices which are not configured with Virtual Chassis configurations, and more frequently on devices configured in Virtual Chassis configurations. This issue is not specific to any particular Junos OS platform. An Indicator of Compromise (IoC) may be seen by reviewing log files for the following error message seen by executing the following show statement: show log messages grep storm</p> <p>Result to look for: /kernel: GENCFG: op 58 (Storm Control Blob) failed; err 1 (Unknown) This issue affects: Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D49 on EX Series; 15.1 versions prior to 15.1R7-S6; 15.1X49 versions prior to 15.1X49-D191, 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3; 17.2 versions prior to 17.2R2-S8, 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S5; 18.2 versions prior to 18.2R2-S6, 18.2R3; 18.3 versions prior to</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			18.3R1-S7, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R1-S5, 18.4R2; 19.1 versions prior to 19.1R1-S4, 19.1R2. CVE ID : CVE-2021-0244								
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-04-2021	6.8	A path traversal vulnerability in the Juniper Networks SRX and vSRX Series may allow an authenticated J-web user to read sensitive system files. This issue affects Juniper Networks Junos OS on SRX and vSRX Series: 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R2-S4, 19.4R3; 20.1 versions prior to 20.1R1-S4, 20.1R2; 20.2 versions prior to 20.2R1-S3, 20.2R2; This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1. CVE ID : CVE-2021-0231	https://kb.juniper.net/JS_A11126	H-JUN-SRX5-040521/680						
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2021	9.3	A Cross-site Scripting (XSS) vulnerability in J-Web on Juniper Networks Junos OS allows an attacker to target another user's session thereby gaining access to the users session. The other user session must be active for the attack to succeed. Once successful, the attacker has the same privileges as the user. If the user has root privileges, the attacker may be able to gain full control of the device. This issue affects: Juniper Networks Junos OS: 12.3	https://kb.juniper.net/JS_A11166	H-JUN-SRX5-040521/681						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 12.3R12-S15 on EX Series; 12.3X48 versions prior to 12.3X48-D95 on SRX Series; 15.1 versions prior to 15.1R7-S6 on EX Series; 15.1X49 versions prior to 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3; 19.1 versions prior to 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S3, 19.2R2; 19.3 versions prior to 19.3R2. CVE ID : CVE-2021-0275		
Incorrect Default Permissions	22-04-2021	4.6	On SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3, devices using tenant services on Juniper Networks Junos OS, due to incorrect default permissions assigned to tenant system administrators a tenant system administrator may inadvertently send their network traffic to one or	https://kb.juniper.net/JS_A11139	H-JUN-SRX5-040521/682

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>more tenants while concurrently modifying the overall device system traffic management, affecting all tenants and the service provider. Further, a tenant may inadvertently receive traffic from another tenant. This issue affects: Juniper Networks Junos OS 18.3 version 18.3R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2; 18.3 versions prior to 18.3R3 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2; 18.4 versions prior to 18.4R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.1 versions prior to 19.1R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3. This issue does not affect: Juniper Networks Junos OS versions prior to 18.3R1.</p> <p>CVE ID : CVE-2021-0246</p>		
srx550					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-04-2021	10	<p>On SRX Series devices configured with UTM services a buffer overflow vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS may allow an attacker to arbitrarily execute code or commands on the target to</p>	https://kb.juniper.net/JS_A11142	H-JUN-SRX5-040521/683

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>take over or otherwise impact the device by sending crafted packets to or through the device. This issue affects: Juniper Networks Junos OS on SRX Series: 15.1X49 versions prior to 15.1X49-D190; 17.4 versions prior to 17.4R2-S9; 17.4R3 and later versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S1; 18.3 versions prior to 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R2-S3, 18.4R3; 19.1 versions prior to 19.1R1-S4, 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. An indicator of compromise can be the following text in the UTM log: RT_UTM: AV_FILE_NOT_SCANNED_PASSED_MT:</p> <p>CVE ID : CVE-2021-0249</p>		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-04-2021	5	<p>An improper restriction of operations within the bounds of a memory buffer vulnerability in Juniper Networks Junos OS J-Web on SRX Series devices allows an attacker to cause Denial of Service (DoS) by sending certain crafted HTTP packets. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. When this issue occurs, web-management, NTP daemon (ntpd) and Layer 2 Control Protocol process (L2CPD)</p>	https://kb.juniper.net/JS_A11122	H-JUN-SRX5-040521/684

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			daemons might crash. This issue affects Juniper Networks Junos OS on SRX Series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2; CVE ID : CVE-2021-0227		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	4.3	A signal handler race condition exists in the Layer 2 Address Learning Daemon (L2ALD) of Juniper Networks Junos OS due to the absence of a specific protection mechanism to avoid a race condition which may allow an attacker to bypass the storm-control feature on devices. This issue is a corner case and only occurs during specific actions taken by an administrator of a device under certain specifics actions which triggers the event. The event occurs less frequently on devices which are not configured with Virtual Chassis configurations, and more frequently on devices	https://kb.juniper.net/JS_A11137	H-JUN-SRX5-040521/685

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>configured in Virtual Chassis configurations. This issue is not specific to any particular Junos OS platform. An Indicator of Compromise (IoC) may be seen by reviewing log files for the following error message seen by executing the following show statement: show log messages grep storm</p> <p>Result to look for: /kernel: GENCFG: op 58 (Storm Control Blob) failed; err 1 (Unknown) This issue affects: Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D49 on EX Series; 15.1 versions prior to 15.1R7-S6; 15.1X49 versions prior to 15.1X49-D191, 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3; 17.2 versions prior to 17.2R2-S8, 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S5; 18.2 versions prior to 18.2R2-S6, 18.2R3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R1-S5, 18.4R2; 19.1 versions prior to 19.1R1-S4, 19.1R2.</p> <p>CVE ID : CVE-2021-0244</p>		

CVSS Scoring Scale	0-1	1-2	2-3	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 Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-04-2021	6.8	A path traversal vulnerability in the Juniper Networks SRX and vSRX Series may allow an authenticated J-web user to read sensitive system files. This issue affects Juniper Networks Junos OS on SRX and vSRX Series: 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R2-S4, 19.4R3; 20.1 versions prior to 20.1R1-S4, 20.1R2; 20.2 versions prior to 20.2R1-S3, 20.2R2; This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1. CVE ID : CVE-2021-0231	https://kb.juniper.net/JS_A11126	H-JUN-SRX5-040521/686
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2021	9.3	A Cross-site Scripting (XSS) vulnerability in J-Web on Juniper Networks Junos OS allows an attacker to target another user's session thereby gaining access to the users session. The other user session must be active for the attack to succeed. Once successful, the attacker has the same privileges as the user. If the user has root privileges, the attacker may be able to gain full control of the device. This issue affects: Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S15 on EX Series; 12.3X48 versions prior to 12.3X48-D95 on SRX Series; 15.1 versions prior to 15.1R7-S6 on EX Series; 15.1X49	https://kb.juniper.net/JS_A11166	H-JUN-SRX5-040521/687

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3; 19.1 versions prior to 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S3, 19.2R2; 19.3 versions prior to 19.3R2. CVE ID : CVE-2021-0275		
srx5600					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-04-2021	10	On SRX Series devices configured with UTM services a buffer overflow vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS may allow an attacker to arbitrarily execute code or commands on the target to take over or otherwise impact the device by sending crafted packets to or through the device. This issue affects: Juniper Networks Junos OS on SRX Series: 15.1X49 versions prior to 15.1X49-D190; 17.4 versions prior to 17.4R2-S9;	https://kb.juniper.net/JS_A11142	H-JUN-SRX5-040521/688

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			17.4R3 and later versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S1; 18.3 versions prior to 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R2-S3, 18.4R3; 19.1 versions prior to 19.1R1-S4, 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. An indicator of compromise can be the following text in the UTM log: RT_UTM: AV_FILE_NOT_SCANNED_PASSED_MT: CVE ID : CVE-2021-0249		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-04-2021	5	An improper restriction of operations within the bounds of a memory buffer vulnerability in Juniper Networks Junos OS J-Web on SRX Series devices allows an attacker to cause Denial of Service (DoS) by sending certain crafted HTTP packets. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. When this issue occurs, web-management, NTP daemon (ntpd) and Layer 2 Control Protocol process (L2CPD) daemons might crash. This issue affects Juniper Networks Junos OS on SRX Series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4,	https://kb.juniper.net/JS_A11122	H-JUN-SRX5-040521/689

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2; CVE ID : CVE-2021-0227		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	4.3	A signal handler race condition exists in the Layer 2 Address Learning Daemon (L2ALD) of Juniper Networks Junos OS due to the absence of a specific protection mechanism to avoid a race condition which may allow an attacker to bypass the storm-control feature on devices. This issue is a corner case and only occurs during specific actions taken by an administrator of a device under certain specifics actions which triggers the event. The event occurs less frequently on devices which are not configured with Virtual Chassis configurations, and more frequently on devices configured in Virtual Chassis configurations. This issue is not specific to any particular Junos OS platform. An Indicator of Compromise (IoC) may be seen by reviewing log files for the following error message seen by executing	https://kb.juniper.net/JS_A11137	H-JUN-SRX5-040521/690

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>the following show statement: show log messages grep storm Result to look for: /kernel: GENCFG: op 58 (Storm Control Blob) failed; err 1 (Unknown) This issue affects: Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D49 on EX Series; 15.1 versions prior to 15.1R7-S6; 15.1X49 versions prior to 15.1X49-D191, 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3; 17.2 versions prior to 17.2R2-S8, 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S5; 18.2 versions prior to 18.2R2-S6, 18.2R3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R1-S5, 18.4R2; 19.1 versions prior to 19.1R1-S4, 19.1R2.</p> <p>CVE ID : CVE-2021-0244</p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-04-2021	6.8	<p>A path traversal vulnerability in the Juniper Networks SRX and vSRX Series may allow an authenticated J-web user to read sensitive system files. This issue affects Juniper Networks Junos OS on SRX and vSRX Series: 19.3</p>	https://kb.juniper.net/JS_A11126	H-JUN-SRX5-040521/691

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R2-S4, 19.4R3; 20.1 versions prior to 20.1R1-S4, 20.1R2; 20.2 versions prior to 20.2R1-S3, 20.2R2; This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1. CVE ID : CVE-2021-0231		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2021	9.3	A Cross-site Scripting (XSS) vulnerability in J-Web on Juniper Networks Junos OS allows an attacker to target another user's session thereby gaining access to the users session. The other user session must be active for the attack to succeed. Once successful, the attacker has the same privileges as the user. If the user has root privileges, the attacker may be able to gain full control of the device. This issue affects: Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S15 on EX Series; 12.3X48 versions prior to 12.3X48-D95 on SRX Series; 15.1 versions prior to 15.1R7-S6 on EX Series; 15.1X49 versions prior to 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to	https://kb.juniper.net/JS_A11166	H-JUN-SRX5-040521/692

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3; 19.1 versions prior to 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S3, 19.2R2; 19.3 versions prior to 19.3R2. CVE ID : CVE-2021-0275		
Incorrect Default Permissions	22-04-2021	4.6	On SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3, devices using tenant services on Juniper Networks Junos OS, due to incorrect default permissions assigned to tenant system administrators a tenant system administrator may inadvertently send their network traffic to one or more tenants while concurrently modifying the overall device system traffic management, affecting all tenants and the service provider. Further, a tenant may inadvertently receive traffic from another tenant. This issue affects: Juniper Networks Junos OS 18.3 version 18.3R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2; 18.3 versions	https://kb.juniper.net/JS_A11139	H-JUN-SRX5-040521/693

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>prior to 18.3R3 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2; 18.4 versions prior to 18.4R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.1 versions prior to 19.1R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3. This issue does not affect: Juniper Networks Junos OS versions prior to 18.3R1.</p> <p>CVE ID : CVE-2021-0246</p>		

srx5800

Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-04-2021	10	<p>On SRX Series devices configured with UTM services a buffer overflow vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS may allow an attacker to arbitrarily execute code or commands on the target to take over or otherwise impact the device by sending crafted packets to or through the device. This issue affects: Juniper Networks Junos OS on SRX Series: 15.1X49 versions prior to 15.1X49-D190; 17.4 versions prior to 17.4R2-S9; 17.4R3 and later versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S1; 18.3 versions prior to 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R2-S3,</p>	https://kb.juniper.net/JS_A11142	H-JUN-SRX5-040521/694
--	------------	----	--	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.4R3; 19.1 versions prior to 19.1R1-S4, 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. An indicator of compromise can be the following text in the UTM log: RT_UTM: AV_FILE_NOT_SCANNED_PASSED_MT: CVE ID : CVE-2021-0249		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-04-2021	5	An improper restriction of operations within the bounds of a memory buffer vulnerability in Juniper Networks Junos OS J-Web on SRX Series devices allows an attacker to cause Denial of Service (DoS) by sending certain crafted HTTP packets. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. When this issue occurs, web-management, NTP daemon (ntpd) and Layer 2 Control Protocol process (L2CPD) daemons might crash. This issue affects Juniper Networks Junos OS on SRX Series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to	https://kb.juniper.net/JS_A11122	H-JUN-SRX5-040521/695

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.3R3; 19.4 versions prior to 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2; CVE ID : CVE-2021-0227		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	4.3	A signal handler race condition exists in the Layer 2 Address Learning Daemon (L2ALD) of Juniper Networks Junos OS due to the absence of a specific protection mechanism to avoid a race condition which may allow an attacker to bypass the storm-control feature on devices. This issue is a corner case and only occurs during specific actions taken by an administrator of a device under certain specific actions which triggers the event. The event occurs less frequently on devices which are not configured with Virtual Chassis configurations, and more frequently on devices configured in Virtual Chassis configurations. This issue is not specific to any particular Junos OS platform. An Indicator of Compromise (IoC) may be seen by reviewing log files for the following error message seen by executing the following show statement: show log messages grep storm Result to look for: /kernel: GENCFG: op 58 (Storm Control Blob) failed; err 1	https://kb.juniper.net/JS_A11137	H-JUN-SRX5-040521/696

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>(Unknown) This issue affects: Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D49 on EX Series; 15.1 versions prior to 15.1R7-S6; 15.1X49 versions prior to 15.1X49-D191, 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3; 17.2 versions prior to 17.2R2-S8, 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S5; 18.2 versions prior to 18.2R2-S6, 18.2R3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R1-S5, 18.4R2; 19.1 versions prior to 19.1R1-S4, 19.1R2.</p> <p>CVE ID : CVE-2021-0244</p>		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-04-2021	6.8	<p>A path traversal vulnerability in the Juniper Networks SRX and vSRX Series may allow an authenticated J-web user to read sensitive system files. This issue affects Juniper Networks Junos OS on SRX and vSRX Series: 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R2-S4, 19.4R3; 20.1 versions prior to 20.1R1-S4, 20.1R2; 20.2 versions prior to 20.2R1-S3,</p>	https://kb.juniper.net/JS_A11126	H-JUN-SRX5-040521/697

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.2R2; This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1. CVE ID : CVE-2021-0231		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2021	9.3	A Cross-site Scripting (XSS) vulnerability in J-Web on Juniper Networks Junos OS allows an attacker to target another user's session thereby gaining access to the users session. The other user session must be active for the attack to succeed. Once successful, the attacker has the same privileges as the user. If the user has root privileges, the attacker may be able to gain full control of the device. This issue affects: Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S15 on EX Series; 12.3X48 versions prior to 12.3X48-D95 on SRX Series; 15.1 versions prior to 15.1R7-S6 on EX Series; 15.1X49 versions prior to 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to	https://kb.juniper.net/JS_A11166	H-JUN-SRX5-040521/698

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.3R1-S7, 18.3R2-S3, 18.3R3-S1; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3; 19.1 versions prior to 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S3, 19.2R2; 19.3 versions prior to 19.3R2. CVE ID : CVE-2021-0275		
Incorrect Default Permissions	22-04-2021	4.6	On SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3, devices using tenant services on Juniper Networks Junos OS, due to incorrect default permissions assigned to tenant system administrators a tenant system administrator may inadvertently send their network traffic to one or more tenants while concurrently modifying the overall device system traffic management, affecting all tenants and the service provider. Further, a tenant may inadvertently receive traffic from another tenant. This issue affects: Juniper Networks Junos OS 18.3 version 18.3R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2; 18.3 versions prior to 18.3R3 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2; 18.4 versions prior to 18.4R2 on SRX1500,	https://kb.juniper.net/JS_A11139	H-JUN-SRX5-040521/699

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.1 versions prior to 19.1R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3. This issue does not affect: Juniper Networks Junos OS versions prior to 18.3R1. CVE ID : CVE-2021-0246		

srx650

Improper Restriction of Operations within the Bounds of a Memory Buffer	22-04-2021	5	An improper restriction of operations within the bounds of a memory buffer vulnerability in Juniper Networks Junos OS J-Web on SRX Series devices allows an attacker to cause Denial of Service (DoS) by sending certain crafted HTTP packets. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. When this issue occurs, web-management, NTP daemon (ntpd) and Layer 2 Control Protocol process (L2CPD) daemons might crash. This issue affects Juniper Networks Junos OS on SRX Series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to	https://kb.juniper.net/JS_A11122	H-JUN-SRX6-040521/700
---	------------	---	--	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2; CVE ID : CVE-2021-0227								
nec											
aterm_wg2600hs											
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-04-2021	10	Aterm WG2600HS firmware Ver1.5.1 and earlier allows an attacker to execute arbitrary OS commands via unspecified vectors. CVE ID : CVE-2021-20711	https://jpn.nec.com/security-info/secinfo/nv21-010.html	H-NEC-ATER-040521/701						
siemens											
scalance_x200-4p_irt											
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-	https://certportal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/702						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code.</p> <p>CVE ID : CVE-2021-25668</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions <	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/703

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution. CVE ID : CVE-2021-25669		

scalance_x201-3p_irt

Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl.	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/704
---------------------	------------	-----	--	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code.</p> <p>CVE ID : CVE-2021-25668</p>		
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE	https://cert-portal.siemens.com	H-SIE-SCAL-040521/705

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
			X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE	ns.com/productcert/pdf/ssa-187092.pdf	

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution.</p> <p>CVE ID : CVE-2021-25669</p>		

scalance_x201-3p_irt_pro

Out-of-bounds Write	22-04-2021	7.5	<p>A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-</p>	<p>https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf</p>	H-SIE-SCAL-040521/706
---------------------	------------	-----	--	--	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code.</p> <p>CVE ID : CVE-2021-25668</p>		
Out-of-bounds Write	22-04-2021	7.5	<p>A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P</p>	https://certportal.siemens.com/productcert/pdf/	H-SIE-SCAL-040521/707

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
			IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2	ssa-187092.pdf	

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution. CVE ID : CVE-2021-25669		
scalance_x202-2_irt					
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All	https://certportal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/708

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code. CVE ID : CVE-2021-25668		
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT	https://certportal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/709

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204- 2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204- 2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206- 1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212- 2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202- 2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution. CVE ID : CVE-2021-25669		
scalance_x202-2p_irt_pro					
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/710

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code.</p> <p>CVE ID : CVE-2021-25668</p>		
Out-of-bounds Write	22-04-2021	7.5	<p>A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All</p>	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/711

CVSS Scoring Scale	0-1	1-2	2-3	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 < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204- 2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204- 2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206- 1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212- 2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202- 2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1),		

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
			SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution. CVE ID : CVE-2021-25669		

scalance_x204_irt

Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl.	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/712
---------------------	------------	-----	--	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code.</p> <p>CVE ID : CVE-2021-25668</p>		
Out-of-bounds Write	22-04-2021	7.5	<p>A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT</p>	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/713

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204- 2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204- 2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206- 1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212- 2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202- 2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution. CVE ID : CVE-2021-25669		
scalance_x204_irt_pro					
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/714

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code.</p> <p>CVE ID : CVE-2021-25668</p>		
Out-of-bounds Write	22-04-2021	7.5	<p>A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1),</p>	<p>https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf</p>	H-SIE-SCAL-040521/715

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution. CVE ID : CVE-2021-25669		
scalance_x204-2					
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl.	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/716

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code. CVE ID : CVE-2021-25668		
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1),	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/717

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			stack. An attacker might leverage this to denial-of-service of the device or remote code execution. CVE ID : CVE-2021-25669		
scalance_x204-2fm					
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-	https://certportal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/718

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code.</p> <p>CVE ID : CVE-2021-25668</p>		
Out-of-bounds Write	22-04-2021	7.5	<p>A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1),</p>	<p>https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf</p>	H-SIE-SCAL-040521/719

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service of the device or remote code execution. CVE ID : CVE-2021-25669		
scalance_x204-2ld					
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/720

CVSS Scoring Scale	0-1	1-2	2-3	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), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code. CVE ID : CVE-2021-25668		
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1),	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/721

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution.</p>		

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-25669		
scalance_x204-2ld_ts					
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE	https://certportal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/722

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code.</p> <p>CVE ID : CVE-2021-25668</p>		
Out-of-bounds Write	22-04-2021	7.5	<p>A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All</p>	<p>https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf</p>	H-SIE-SCAL-040521/723

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution.</p> <p>CVE ID : CVE-2021-25669</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
scalance_x204-2ts											
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/724						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code.</p> <p>CVE ID : CVE-2021-25668</p>		
Out-of-bounds Write	22-04-2021	7.5	<p>A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions),</p>	<p>https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf</p>	H-SIE-SCAL-040521/725

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution. CVE ID : CVE-2021-25669							
scalance_x206-1										
Out-of-	22-04-2021	7.5	A vulnerability has been	https://cert-	H-SIE-SCAL-					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204	portal.siemens.com/productcert/pdf/ssa-187092.pdf	040521/726

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code. CVE ID : CVE-2021-25668		
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/727

CVSS Scoring Scale	0-1	1-2	2-3	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), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution. CVE ID : CVE-2021-25669		
scalance_x206-1ld					
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions <	https://cert-portal.siemens.com/prod	H-SIE-SCAL-040521/728

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions <	uctcert/pdf/ssa-187092.pdf	

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code. CVE ID : CVE-2021-25668		
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/729

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution.</p> <p>CVE ID : CVE-2021-25669</p>		
scalance_x208					
Out-of-bounds Write	22-04-2021	7.5	<p>A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1),</p>	https://certportal.siemens.com/productcert/pdf/ssa-	H-SIE-SCAL-040521/730

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant)	187092.pdf	

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code. CVE ID : CVE-2021-25668		
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-	https://certportal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/731

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution.</p> <p>CVE ID : CVE-2021-25669</p>		
scalance_x208pro					
Out-of-bounds Write	22-04-2021	7.5	<p>A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1),</p>	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/732

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All		

CVSS Scoring Scale	0-1	1-2	2-3	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 < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code. CVE ID : CVE-2021-25668		
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions),	https://certportal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/733

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution.</p> <p>CVE ID : CVE-2021-25669</p>		
scalance_x212-2					
Out-of-bounds Write	22-04-2021	7.5	<p>A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1),</p>	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/734

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
			SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All		

CVSS Scoring Scale	0-1	1-2	2-3	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), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code. CVE ID : CVE-2021-25668		
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/735

CVSS Scoring Scale	0-1	1-2	2-3	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), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution. CVE ID : CVE-2021-25669		
scalance_x212-2ld					
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant)	https://certportal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/736

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect		

CVSS Scoring Scale	0-1	1-2	2-3	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 of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code. CVE ID : CVE-2021-25668		
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions),	https://certportal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/737

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution.</p> <p>CVE ID : CVE-2021-25669</p>		
scalance_x216					
Out-of-bounds Write	22-04-2021	7.5	<p>A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT</p>	<p>https://certportal.siemens.com/productcert/pdf/ssa-187092.pdf</p>	H-SIE-SCAL-040521/738

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204- 2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204- 2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206- 1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212- 2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202- 2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver		

CVSS Scoring Scale	0-1	1-2	2-3	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 result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code. CVE ID : CVE-2021-25668		
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/739

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution. CVE ID : CVE-2021-25669		
scalance_x224					
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/740

CVSS Scoring Scale	0-1	1-2	2-3	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 < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker		

CVSS Scoring Scale	0-1	1-2	2-3	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 leverage this to cause denial-of-service on the device and potentially remotely execute code. CVE ID : CVE-2021-25668		
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/741

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution.</p> <p>CVE ID : CVE-2021-25669</p>		

scalance_xf201-3p_irt

Out-of-bounds Write	22-04-2021	7.5	<p>A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO</p>	<p>https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf</p>	H-SIE-SCAL-040521/742
---------------------	------------	-----	--	--	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device and potentially remotely execute code. CVE ID : CVE-2021-25668		
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/743

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution. CVE ID : CVE-2021-25669		

scalance_xf202-2p_irt

Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl.	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/744
---------------------	------------	-----	---	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code.		

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-25668								
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/745						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution.</p> <p>CVE ID : CVE-2021-25669</p>		

scalance_xf204

Out-of-bounds Write	22-04-2021	7.5	<p>A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions),</p>	<p>https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf</p>	H-SIE-SCAL-040521/746
---------------------	------------	-----	--	--	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code.</p> <p>CVE ID : CVE-2021-25668</p>		
Out-of-	22-04-2021	7.5	A vulnerability has been	https://cert-	H-SIE-SCAL-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204	portal.siemens.com/productcert/pdf/ssa-187092.pdf	040521/747

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution. CVE ID : CVE-2021-25669		

scalance_xf204_irt

Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/748
---------------------	------------	-----	---	---	-----------------------

CVSS Scoring Scale	0-1	1-2	2-3	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), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code. CVE ID : CVE-2021-25668		
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions <	https://cert-portal.siemens.com/prod	H-SIE-SCAL-040521/749

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
			5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions <	uctcert/pdf/ssa-187092.pdf	

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution. CVE ID : CVE-2021-25669		

scalance_xf204-2

Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/750
---------------------	------------	-----	---	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code.</p> <p>CVE ID : CVE-2021-25668</p>		
Out-of-bounds Write	22-04-2021	7.5	<p>A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1),</p>	https://cert-portal.siemens.com/productcert/pdf/ssa-	H-SIE-SCAL-040521/751

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant)	187092.pdf	

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution. CVE ID : CVE-2021-25669		

scalance_xf204-2ba_irt

Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/752
---------------------	------------	-----	--	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code.</p> <p>CVE ID : CVE-2021-25668</p>		
Out-of-bounds Write	22-04-2021	7.5	<p>A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1),</p>	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/753

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All		

CVSS Scoring Scale	0-1	1-2	2-3	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 < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution. CVE ID : CVE-2021-25669		

scalance_xf206-1

Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions),	https://certportal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/754
---------------------	------------	-----	---	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code.</p> <p>CVE ID : CVE-2021-25668</p>		
Out-of-bounds Write	22-04-2021	7.5	<p>A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1),</p>	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/755

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All		

CVSS Scoring Scale	0-1	1-2	2-3	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), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution. CVE ID : CVE-2021-25669		

scalance_xf208

Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/756
---------------------	------------	-----	---	---	-----------------------

CVSS Scoring Scale	0-1	1-2	2-3	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), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code. CVE ID : CVE-2021-25668		
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant)	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	H-SIE-SCAL-040521/757

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect		

CVSS Scoring Scale	0-1	1-2	2-3	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 of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution. CVE ID : CVE-2021-25669							
simotics_connect_400										
Use of Insufficiently Random Values	22-04-2021	5	A vulnerability has been identified in Nucleus 4 (All versions < V4.1.0), Nucleus NET (All versions), Nucleus RTOS (versions including affected DNS modules), Nucleus ReadyStart (All versions < V2017.02.3), Nucleus Source Code (versions including affected DNS modules), SIMOTICS CONNECT 400 (All versions < V0.5.0.0), SIMOTICS CONNECT 400 (All versions >= V0.5.0.0), VSTAR (versions including affected DNS modules). The DNS client does not properly randomize DNS transaction IDs. That could allow an attacker to poison the DNS cache or spoof DNS resolving. CVE ID : CVE-2021-25677	https://cert-portal.siemens.com/productcert/pdf/ssa-705111.pdf , https://cert-portal.siemens.com/productcert/pdf/ssa-669158.pdf	H-SIE-SIMO-040521/758					
tendacn										
g0										
Improper Neutralization of Special Elements used in an OS Command ('OS	16-04-2021	10	Command Injection in Tenda G0 routers with firmware versions v15.11.0.6(9039)_CN and v15.11.0.5(5876)_CN , and Tenda G1 and G3 routers with firmware versions	N/A	H-TEN-G0-040521/759					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			v15.11.0.17(9502)_CN or v15.11.0.16(9024)_CN allows remote attackers to execute arbitrary OS commands via a crafted action/setDebugCfg request. This occurs because the "formSetDebugCfg" function executes glibc's system function with untrusted input. CVE ID : CVE-2021-27691		
g1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-04-2021	10	Command Injection in Tenda G0 routers with firmware versions v15.11.0.6(9039)_CN and v15.11.0.5(5876)_CN , and Tenda G1 and G3 routers with firmware versions v15.11.0.17(9502)_CN or v15.11.0.16(9024)_CN allows remote attackers to execute arbitrary OS commands via a crafted action/setDebugCfg request. This occurs because the "formSetDebugCfg" function executes glibc's system function with untrusted input. CVE ID : CVE-2021-27691	N/A	H-TEN-G1-040521/760
Improper Neutralization of Special Elements used in an OS Command ('OS Command	16-04-2021	10	Command Injection in Tenda G1 and G3 routers with firmware versions v15.11.0.17(9502)_CN or v15.11.0.16(9024)_CN allows remote attackers to execute arbitrary OS commands via a crafted	N/A	H-TEN-G1-040521/761

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			"action/umountUSBPartitio n" request. This occurs because the "formSetUSBPartitionUmou nt" function executes the "doSystemCmd" function with untrusted input. CVE ID : CVE-2021-27692		
g3					
Improper Neutralizatio n of Special Elements used in an OS Command (OS Command Injection')	16-04-2021	10	Command Injection in Tenda G0 routers with firmware versions v15.11.0.6(9039)_CN and v15.11.0.5(5876)_CN , and Tenda G1 and G3 routers with firmware versions v15.11.0.17(9502)_CN or v15.11.0.16(9024)_CN allows remote attackers to execute arbitrary OS commands via a crafted action/setDebugCfg request. This occurs because the "formSetDebugCfg" function executes glibc's system function with untrusted input. CVE ID : CVE-2021-27691	N/A	H-TEN-G3- 040521/762
Improper Neutralizatio n of Special Elements used in an OS Command (OS Command Injection')	16-04-2021	10	Command Injection in Tenda G1 and G3 routers with firmware versions v15.11.0.17(9502)_CN or v15.11.0.16(9024)_CN allows remote attackers to execute arbitrary OS commands via a crafted "action/umountUSBPartitio n" request. This occurs because the "formSetUSBPartitionUmou nt" function executes the	N/A	H-TEN-G3- 040521/763

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			"doSystemCmd" function with untrusted input. CVE ID : CVE-2021-27692								
Operating System											
alpinelinux											
apk-tools											
Out-of-bounds Read	21-04-2021	5	In Alpine Linux apk-tools before 2.12.5, the tarball parser allows a buffer overflow and crash. CVE ID : CVE-2021-30139	N/A	O-ALP-APK--040521/764						
amazon											
freertos											
Integer Overflow or Wraparound	22-04-2021	7.5	The kernel in Amazon Web Services FreeRTOS before 10.4.3 has an integer overflow in queue.c for queue creation. CVE ID : CVE-2021-31571	https://github.com/FreeRTOS/FreeRTOS-Kernel/commit/c7a9a01c94987082b223d3e59969ede64363da63 , https://github.com/FreeRTOS/FreeRTOS-Kernel/commit/47338393f1f79558f6144213409f09f81d7c4837	O-AMA-FREE-040521/765						
Integer Overflow or Wraparound	22-04-2021	7.5	The kernel in Amazon Web Services FreeRTOS before 10.4.3 has an integer overflow in stream_buffer.c for a stream buffer. CVE ID : CVE-2021-31572	https://github.com/FreeRTOS/FreeRTOS-Kernel/commit/c7a9a01c94987082b223d3e5996	O-AMA-FREE-040521/766						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				9ede64363da63, https://github.com/FreeRTOS/FreeRTOS-Kernel/commit/d05b9c123f2bf9090bce386a244fc934ae44db5b	
apple					
mac_os_x					
Use After Free	26-04-2021	6.8	Use after free in Blink in Google Chrome on OS X prior to 90.0.4430.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-21204	N/A	O-APP-MAC_-040521/767
aterm					
wg2600hs_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-04-2021	4.3	Cross-site scripting vulnerability in Aterm WG2600HS firmware Ver1.5.1 and earlier allows remote attackers to inject an arbitrary script via unspecified vectors. CVE ID : CVE-2021-20710	N/A	O-ATE-WG26-040521/768
canonical					
ubuntu_linux					
Double Free	17-04-2021	7.2	Shiftfs, an out-of-tree stacking file system included in Ubuntu Linux kernels, did not properly handle faults occurring during copy_from_user()	https://git.launchpad.net/~ubuntu-kernel/ubuntu/+source/linux/+git/fo	O-CAN-UBUN-040521/769

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			correctly. These could lead to either a double-free situation or memory not being freed at all. An attacker could use this to cause a denial of service (kernel memory exhaustion) or gain privileges via executing arbitrary code. AKA ZDI-CAN-13562. CVE ID : CVE-2021-3492	cal/commit/?id=25c891a949bf918b59cbc6e4932015ba4c35c333, https://git.launchpad.net/~ubuntu-kernel/ubuntu/+source/linux/+git/focal/commit/?id=8fee52ab9da87d82bc6de9ebb3480fff9b4d53e6	
Improper Privilege Management	17-04-2021	7.2	The overlayfs implementation in the linux kernel did not properly validate with respect to user namespaces the setting of file capabilities on files in an underlying file system. Due to the combination of unprivileged user namespaces along with a patch carried in the Ubuntu kernel to allow unprivileged overlay mounts, an attacker could use this to gain elevated privileges. CVE ID : CVE-2021-3493	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=7c03e2cda4a584cadc398e8f6641ca9988a39d52 , https://ubuntu.com/security/notices/USN-4917-1	O-CAN-UBUN-040521/770
debian					
debian_linux					
N/A	26-04-2021	5.8	Insufficient policy enforcement in navigation in Google Chrome on iOS prior to 90.0.4430.72 allowed a remote attacker to bypass navigation	N/A	O-DEB-DEBI-040521/771

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			restrictions via a crafted HTML page. CVE ID : CVE-2021-21205		
Use After Free	26-04-2021	6.8	Use after free in IndexedDB in Google Chrome prior to 90.0.4430.72 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension. CVE ID : CVE-2021-21207	N/A	O-DEB-DEBI-040521/772
Improper Input Validation	26-04-2021	4.3	Insufficient data validation in QR scanner in Google Chrome on iOS prior to 90.0.4430.72 allowed an attacker displaying a QR code to perform domain spoofing via a crafted QR code. CVE ID : CVE-2021-21208	N/A	O-DEB-DEBI-040521/773
Improper Input Validation	26-04-2021	4.3	Insufficient validation of untrusted input in Mojo in Google Chrome prior to 90.0.4430.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. CVE ID : CVE-2021-21221	N/A	O-DEB-DEBI-040521/774
Out-of-bounds Write	26-04-2021	4.3	Heap buffer overflow in V8 in Google Chrome prior to 90.0.4430.85 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. CVE ID : CVE-2021-21222	N/A	O-DEB-DEBI-040521/775

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	26-04-2021	6.8	Integer overflow in Mojo in Google Chrome prior to 90.0.4430.85 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2021-21223	N/A	O-DEB-DEBI-040521/776
Access of Resource Using Incompatible Type ('Type Confusion')	26-04-2021	6.8	Type confusion in V8 in Google Chrome prior to 90.0.4430.85 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. CVE ID : CVE-2021-21224	N/A	O-DEB-DEBI-040521/777
Improper Restriction of Operations within the Bounds of a Memory Buffer	26-04-2021	6.8	Out of bounds memory access in V8 in Google Chrome prior to 90.0.4430.85 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-21225	N/A	O-DEB-DEBI-040521/778
Origin Validation Error	26-04-2021	4.3	Inappropriate implementation in storage in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. CVE ID : CVE-2021-21209	N/A	O-DEB-DEBI-040521/779
Origin Validation Error	26-04-2021	4.3	Inappropriate implementation in Navigation in Google Chrome on iOS prior to 90.0.4430.72 allowed a remote attacker to leak cross-origin data via a	N/A	O-DEB-DEBI-040521/780

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted HTML page. CVE ID : CVE-2021-21211		
Use of Uninitialized Resource	26-04-2021	4.3	Uninitialized data in PDFium in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted PDF file. CVE ID : CVE-2021-21218	N/A	O-DEB-DEBI-040521/781
Use After Free	26-04-2021	6.8	Use after free in WebMIDI in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-21213	N/A	O-DEB-DEBI-040521/782
Use After Free	26-04-2021	6.8	Use after free in Network API in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to potentially exploit heap corruption via a crafted Chrome Extension. CVE ID : CVE-2021-21214	N/A	O-DEB-DEBI-040521/783
Authentication Bypass by Spoofing	26-04-2021	4.3	Inappropriate implementation in Autofill in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to spoof security UI via a crafted HTML page. CVE ID : CVE-2021-21215	https://chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop_14.html , https://crbug.com/1172533	O-DEB-DEBI-040521/784
Authentication Bypass by	26-04-2021	4.3	Inappropriate implementation in Autofill	https://crbug.com/1173	O-DEB-DEBI-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Spoofing			in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to spoof security UI via a crafted HTML page. CVE ID : CVE-2021-21216	297, https://chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop_14.html	040521/785
Exposure of Resource to Wrong Sphere	26-04-2021	4.3	Inappropriate implementation in Network in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to potentially access local UDP ports via a crafted HTML page. CVE ID : CVE-2021-21210	N/A	O-DEB-DEBI-040521/786
N/A	26-04-2021	4.3	Incorrect security UI in Network Config UI in Google Chrome on ChromeOS prior to 90.0.4430.72 allowed a remote attacker to potentially compromise WiFi connection security via a malicious WAP. CVE ID : CVE-2021-21212	N/A	O-DEB-DEBI-040521/787
Exposure of Sensitive Information to an Unauthorized Actor	26-04-2021	4.3	Uninitialized data in PDFium in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted PDF file. CVE ID : CVE-2021-21217	https://crbug.com/1166462 , https://chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop_14.html	O-DEB-DEBI-040521/788
Exposure of Sensitive	26-04-2021	4.3	Uninitialized data in PDFium in Google Chrome	N/A	O-DEB-DEBI-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information to an Unauthorized Actor			prior to 90.0.4430.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted PDF file. CVE ID : CVE-2021-21219		040521/789
Use After Free	26-04-2021	6.8	Use after free in navigation in Google Chrome prior to 90.0.4430.85 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2021-21226	N/A	O-DEB-DEBI-040521/790
Use After Free	19-04-2021	6.8	GStreamer before 1.18.4 might access already-freed memory in error code paths when demuxing certain malformed Matroska files. CVE ID : CVE-2021-3497	https://gstreamer.freedesktop.org/security/sa-2021-0002.html , https://bugzilla.redhat.com/show_bug.cgi?id=1945339	O-DEB-DEBI-040521/791
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-04-2021	6.8	GStreamer before 1.18.4 might cause heap corruption when parsing certain malformed Matroska files. CVE ID : CVE-2021-3498	https://gstreamer.freedesktop.org/security/sa-2021-0003.html , https://bugzilla.redhat.com/show_bug.cgi?id=1945342	O-DEB-DEBI-040521/792
fedoraproject					
fedora					
Concurrent	22-04-2021	6.9	A race condition in Linux	https://git.k	O-FED-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Execution using Shared Resource with Improper Synchronization ('Race Condition')			kernel SCTP sockets (net/sctp/socket.c) before 5.12-rc8 can lead to kernel privilege escalation from the context of a network service or an unprivileged process. If sctp_destroy_sock is called without sock_net(sk)->sctp.addr_wq_lock then an element is removed from the auto_asconf_splist list without any proper locking. This can be exploited by an attacker with network service privileges to escalate to root or from the context of an unprivileged user directly if a BPF_CGROUP_INET_SOCK_CREATE is attached which denies creation of some SCTP socket. CVE ID : CVE-2021-23133	ernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=b166a20b07382b8bc1dcee2a448715c9c2c81b5b, https://www.openwall.com/lists/oss-security/2021/04/18/2	FEDO-040521/793
Improper Restriction of XML External Entity Reference	21-04-2021	5	The REXML gem before 3.2.5 in Ruby before 2.6.7, 2.7.x before 2.7.3, and 3.x before 3.0.1 does not properly address XML round-trip issues. An incorrect document can be produced after parsing and serializing. CVE ID : CVE-2021-28965	https://www.ruby-lang.org/en/news/2021/04/05/xml-round-trip-vulnerability-in-rexml-cve-2021-28965/	O-FED-FEDO-040521/794
Out-of-bounds Read	20-04-2021	2.1	An issue was discovered in the Linux kernel through 5.11.x. kernel/bpf/verifier.c performs undesirable out-of-bounds speculation on pointer arithmetic, leading to side-channel attacks that defeat Spectre mitigations and obtain sensitive	https://www.kernel.org , https://www.openwall.com/lists/oss-security/2021/04/18/4	O-FED-FEDO-040521/795

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information from kernel memory. Specifically, for sequences of pointer arithmetic operations, the pointer modification performed by the first operation is not correctly accounted for when restricting subsequent operations. CVE ID : CVE-2021-29155		
fibaro					
home_center_2_firmware					
Incorrect Authorization	19-04-2021	7.8	In Fibaro Home Center 2 and Lite devices with firmware version 4.600 and older an internal management service is accessible on port 8000 and some API endpoints could be accessed without authentication to trigger a shutdown, a reboot or a reboot into recovery mode. CVE ID : CVE-2021-20990	https://www.iot-inspector.com/blog/advisory-fibaro-home-center/	O-FIB-HOME-040521/796
Cleartext Transmission of Sensitive Information	19-04-2021	5	In Fibaro Home Center 2 and Lite devices in all versions provide a web based management interface over unencrypted HTTP protocol. Communication between the user and the device can be eavesdropped to hijack sessions, tokens and passwords. CVE ID : CVE-2021-20992	https://www.iot-inspector.com/blog/advisory-fibaro-home-center/	O-FIB-HOME-040521/797
Missing Authorization	19-04-2021	4.3	Fibaro Home Center 2 and Lite devices with firmware version 4.600 and older initiate SSH connections to	https://www.iot-inspector.com/blog/advisory-fibaro-home-center/	O-FIB-HOME-040521/798

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			the Fibaro cloud to provide remote access and remote support capabilities. This connection can be intercepted using DNS spoofing attack and a device initiated remote port-forward channel can be used to connect to the web management interface. Knowledge of authorization credentials to the management interface is required to perform any further actions. CVE ID : CVE-2021-20989	sory-fibaro-home-center/							
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-04-2021	9	In Fibaro Home Center 2 and Lite devices with firmware version 4.540 and older an authenticated user can run commands as root user using a command injection vulnerability. CVE ID : CVE-2021-20991	https://www.iot-inspector.com/blog/advisory-fibaro-home-center/	O-FIB-HOME-040521/799						
home_center_lite_firmware											
Incorrect Authorization	19-04-2021	7.8	In Fibaro Home Center 2 and Lite devices with firmware version 4.600 and older an internal management service is accessible on port 8000 and some API endpoints could be accessed without authentication to trigger a shutdown, a reboot or a reboot into recovery mode. CVE ID : CVE-2021-20990	https://www.iot-inspector.com/blog/advisory-fibaro-home-center/	O-FIB-HOME-040521/800						
Cleartext Transmission of Sensitive Information	19-04-2021	5	In Fibaro Home Center 2 and Lite devices in all versions provide a web based management	https://www.iot-inspector.com/blog/advi	O-FIB-HOME-040521/801						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			interface over unencrypted HTTP protocol. Communication between the user and the device can be eavesdropped to hijack sessions, tokens and passwords. CVE ID : CVE-2021-20992	sory-fibaro-home-center/						
Missing Authorization	19-04-2021	4.3	Fibaro Home Center 2 and Lite devices with firmware version 4.600 and older initiate SSH connections to the Fibaro cloud to provide remote access and remote support capabilities. This connection can be intercepted using DNS spoofing attack and a device initiated remote port-forward channel can be used to connect to the web management interface. Knowledge of authorization credentials to the management interface is required to perform any further actions. CVE ID : CVE-2021-20989	https://www.iot-inspector.com/blog/advisory-fibaro-home-center/	O-FIB-HOME-040521/802					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-04-2021	9	In Fibaro Home Center 2 and Lite devices with firmware version 4.540 and older an authenticated user can run commands as root user using a command injection vulnerability. CVE ID : CVE-2021-20991	https://www.iot-inspector.com/blog/advisory-fibaro-home-center/	O-FIB-HOME-040521/803					
hp										
hp-ux										
Out-of-bounds Write	30-04-2021	4.6	IBM Informix Dynamic Server 14.10 is vulnerable to a stack based buffer	https://exchange.xforce.ibmcloud.com	O-HP-HP-U-040521/804					
CVSS Scoring Scale	0-1	1-2	2-3	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, caused by improper bounds checking. A local privileged user could overflow a buffer and execute arbitrary code on the system or cause a denial of service condition. IBM X-Force ID: 198366. CVE ID : CVE-2021-20515	m/vulnerabilities/198366, https://www.ibm.com/support/pages/node/6448568							
ibm											
aix											
Out-of-bounds Write	30-04-2021	4.6	IBM Informix Dynamic Server 14.10 is vulnerable to a stack based buffer overflow, caused by improper bounds checking. A local privileged user could overflow a buffer and execute arbitrary code on the system or cause a denial of service condition. IBM X-Force ID: 198366. CVE ID : CVE-2021-20515	https://exchange.xforce.ibmcloud.com/vulnerabilities/198366 , https://www.ibm.com/support/pages/node/6448568	O-IBM-AIX-040521/805						
i											
Uncontrolled Resource Consumption	21-04-2021	6.4	IBM i 7.1, 7.2, 7.3, and 7.4 SMTP allows a network attacker to send emails to non-existent local-domain recipients to the SMTP server, caused by using a non-default configuration. An attacker could exploit this vulnerability to consume unnecessary network bandwidth and disk space, and allow remote attackers to send spam email. IBM X-Force ID: 198056. CVE ID : CVE-2021-20501	https://exchange.xforce.ibmcloud.com/vulnerabilities/198056 , https://www.ibm.com/support/pages/node/6445505	O-IBM-I-040521/806						
jtek											
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
2port-efr_thu-6404_firmware											
Improper Resource Shutdown or Release	19-04-2021	5	If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters. CVE ID : CVE-2021-27458	N/A	O-JTE-2POR-040521/807						
fl\\et-t-v2h_thu-6289_firmware											
Improper Resource	19-04-2021	5	If Ethernet communication of the JTEKT Corporation	N/A	O-JTE-FL\\-						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Shutdown or Release			<p>TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters.</p> <p>CVE ID : CVE-2021-27458</p>		040521/808
pc10b_tcc-1021_firmware					
Improper Resource Shutdown or Release	19-04-2021	5	<p>If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All</p>	N/A	O-JTE-PC10-040521/809

CVSS Scoring Scale	0-1	1-2	2-3	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, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters. CVE ID : CVE-2021-27458		
pc10b-e\\c_tcu-6521_firmware					
Improper Resource Shutdown or Release	19-04-2021	5	If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions,	N/A	O-JTE-PC10-040521/810

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters.</p> <p>CVE ID : CVE-2021-27458</p>		
pc10b-p_tcc-6373_firmware					
Improper Resource Shutdown or Release	19-04-2021	5	<p>If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P</p>	N/A	O-JTE-PC10-040521/811

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters.</p> <p>CVE ID : CVE-2021-27458</p>		
pc10e_tcc-4737_firmware					
Improper Resource Shutdown or Release	19-04-2021	5	<p>If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-</p>	N/A	O-JTE-PC10-040521/812

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters.</p> <p>CVE ID : CVE-2021-27458</p>		

pc10g-cpu_tcc-6353_firmware

Improper Resource Shutdown or Release	19-04-2021	5	<p>If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus</p>	N/A	O-JTE-PC10-040521/813
---------------------------------------	------------	---	---	-----	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters.</p> <p>CVE ID : CVE-2021-27458</p>		
pc10ge_tcc-6464_firmware					
Improper Resource Shutdown or Release	19-04-2021	5	<p>If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-</p>	N/A	O-JTE-PC10-040521/814

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters.</p> <p>CVE ID : CVE-2021-27458</p>		

pc10p_tcc-6372_firmware

Improper Resource Shutdown or Release	19-04-2021	5	<p>If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All</p>	N/A	O-JTE-PC10-040521/815
---------------------------------------	------------	---	---	-----	-----------------------

CVSS Scoring Scale	0-1	1-2	2-3	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, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters. CVE ID : CVE-2021-27458		

pc10p-dp_tcc-6726_firmware

Improper Resource Shutdown or Release	19-04-2021	5	If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All	N/A	O-JTE-PC10-040521/816
---------------------------------------	------------	---	--	-----	-----------------------

CVSS Scoring Scale	0-1	1-2	2-3	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; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters. CVE ID : CVE-2021-27458		
pc10p-dp-io_tcc-6752_firmware					
Improper Resource Shutdown or Release	19-04-2021	5	If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All	N/A	O-JTE-PC10-040521/817

CVSS Scoring Scale	0-1	1-2	2-3	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, 2PORT-EFR THU-6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters. CVE ID : CVE-2021-27458		
plus_2p-efr_tcu-6929_firmware					
Improper Resource Shutdown or Release	19-04-2021	5	If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-6404: All versions) are left in an open state by an	N/A	O-JTE-PLUS-040521/818

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters. CVE ID : CVE-2021-27458		
plus_bus-ex_tcu-6900_firmware					
Improper Resource Shutdown or Release	19-04-2021	5	If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other	N/A	O-JTE-PLUS-040521/819

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						
			devices, depending on the settings of the link parameters. CVE ID : CVE-2021-27458								
plus_cpu_tcc-6740_firmware											
Improper Resource Shutdown or Release	19-04-2021	5	If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters.	N/A	O-JTE-PLUS-040521/820						
CVSS Scoring Scale		0-1	1-2	2-3	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-2021-27458		
plus_efr_tcu-6743_firmware					
Improper Resource Shutdown or Release	19-04-2021	5	<p>If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters.</p> <p>CVE ID : CVE-2021-27458</p>	N/A	O-JTE-PLUS-040521/821
plus_efr2_tcu-6859_firmware					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Resource Shutdown or Release	19-04-2021	5	<p>If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters.</p> <p>CVE ID : CVE-2021-27458</p>	N/A	O-JTE-PLUS-040521/822
plus_ex_tcu-6741_firmware					
Improper Resource Shutdown or	19-04-2021	5	If Ethernet communication of the JTEKT Corporation TOYOPUC product series'	N/A	O-JTE-PLUS-040521/823

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Release			<p>(TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters.</p> <p>CVE ID : CVE-2021-27458</p>		
plus_ex2_tcu-6858_firmware					
Improper Resource Shutdown or Release	19-04-2021	5	<p>If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-</p>	N/A	O-JTE-PLUS-040521/824

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters. CVE ID : CVE-2021-27458							
juniper										
junos										
Improper Input Validation	22-04-2021	3.3	A vulnerability in the distributed or centralized periodic packet management daemon (PPMD) of Juniper Networks Junos OS may cause receipt of a malformed packet to crash	https://kb.juniper.net/JS_A11117	O-JUN-JUNO-040521/825					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>and restart the PPMD process, leading to network destabilization, service interruption, and a Denial of Service (DoS) condition. Continued receipt and processing of these malformed packets will repeatedly crash the PPMD process and sustain the Denial of Service (DoS) condition. Due to the nature of the specifically crafted packet, exploitation of this issue requires direct, adjacent connectivity to the vulnerable component. This issue affects Juniper Networks Junos OS: 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S12, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S5, 19.2R3-S1; 19.3 versions prior to 19.3R2-S5, 19.3R3-S1; 19.4 versions prior to 19.4R2-S2, 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R1-S2, 20.2R2.</p> <p>CVE ID : CVE-2021-0214</p>		
Uncontrolled Resource Consumption	22-04-2021	5	<p>A vulnerability in Juniper Networks Junos OS ACX500 Series, ACX4000 Series, may</p>	https://kb.juniper.net/JS_A11128	O-JUN-JUNO-040521/826

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to cause a Denial of Service (DoS) by sending a high rate of specific packets to the device, resulting in a Forwarding Engine Board (FFEB) crash. Continued receipt of these packets will sustain the Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS on ACX500 Series, ACX4000 Series: 17.4 versions prior to 17.4R3-S2. CVE ID : CVE-2021-0233		
Improper Initialization	22-04-2021	5	Due to an improper Initialization vulnerability on Juniper Networks Junos OS QFX5100-96S devices with QFX 5e Series image installed, ddos-protection configuration changes will not take effect beyond the default DDoS (Distributed Denial of Service) settings when configured from the CLI. The DDoS protection (jddosd) daemon allows the device to continue to function while protecting the packet forwarding engine (PFE) during the DDoS attack. When this issue occurs, the default DDoS settings within the PFE apply, as CPU bound packets will be throttled and dropped in the PFE when the limits are exceeded. To check if the device has this issue, the administrator can execute the following command to	https://kb.juniper.net/JS_A11129	O-JUN-JUNO-040521/827

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
			<p>monitor the status of DDoS protection: user@device> show ddos-protection protocols error: the ddos-protection subsystem is not running This issue affects only QFX5100-96S devices. No other products or platforms are affected by this issue. This issue affects: Juniper Networks Junos OS on QFX5100-96S: 17.3 versions prior to 17.3R3-S10; 17.4 versions prior to 17.4R3-S4; 18.1 versions prior to 18.1R3-S10; 18.2 versions prior to 18.2R3-S3; 18.3 versions prior to 18.3R3-S2; 18.4 versions prior to 18.4R2-S4, 18.4R3-S1; 19.1 versions prior to 19.1R3, 19.1R3-S4; 19.2 versions prior to 19.2R2; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2;</p> <p>CVE ID : CVE-2021-0234</p>		
Incorrect Default Permissions	22-04-2021	4.6	<p>On SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3, vSRX Series devices using tenant services on Juniper Networks Junos OS, due to incorrect permission scheme assigned to tenant system administrators, a tenant system administrator may inadvertently send their network traffic to one or more tenants while concurrently modifying the</p>	https://kb.juniper.net/JS_A11130	O-JUN-JUNO-040521/828

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>overall device system traffic management, affecting all tenants and the service provider. Further, a tenant may inadvertently receive traffic from another tenant. This issue affects: Juniper Networks Junos OS 18.3 version 18.3R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2; 18.4 version 18.4R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.1 versions 19.1R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.3 versions prior to 19.3R3-S2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 20.1 versions prior to 20.1R2, 20.1R3 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series; 20.2 versions prior to</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>20.2R2-S1, 20.2R3 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series; 20.3 versions prior to 20.3R1-S2, 20.3R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series; 20.4 versions prior to 20.4R1, 20.4R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3 vSRX Series. This issue does not affect Juniper Networks Junos OS versions prior to 18.3R1.</p> <p>CVE ID : CVE-2021-0235</p>		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-04-2021	10	<p>On SRX Series devices configured with UTM services a buffer overflow vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS may allow an attacker to arbitrarily execute code or commands on the target to take over or otherwise impact the device by sending crafted packets to or through the device. This issue affects: Juniper Networks Junos OS on SRX Series: 15.1X49 versions prior to 15.1X49-D190; 17.4 versions prior to 17.4R2-S9; 17.4R3 and later versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S1; 18.3 versions prior to</p>	https://kb.juniper.net/JS_A11142	O-JUN-JUNO-040521/829

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R2-S3, 18.4R3; 19.1 versions prior to 19.1R1-S4, 19.1R2; 19.2 versions prior to 19.2R1-S1, 19.2R2. An indicator of compromise can be the following text in the UTM log: RT_UTM: AV_FILE_NOT_SCANNED_PASSED_MT: CVE ID : CVE-2021-0249		
N/A	22-04-2021	5	In segment routing traffic engineering (SRTE) environments where the BGP Monitoring Protocol (BMP) feature is enable, a vulnerability in the Routing Protocol Daemon (RPD) process of Juniper Networks Junos OS allows an attacker to send a specific crafted BGP update message causing the RPD service to core, creating a Denial of Service (DoS) Condition. Continued receipt and processing of this update message will create a sustained Denial of Service (DoS) condition. This issue affects IPv4 and IPv6 environments. This issue affects: Juniper Networks Junos OS 17.4 versions 17.4R1 and above prior to 17.4R2-S6, 17.4R3; 18.1 versions prior to 18.1R3-S7; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3; 18.4 versions prior	https://kb.juniper.net/JS_A11143	O-JUN-JUNO-040521/830

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to 18.4R1-S5, 18.4R2-S3, 18.4R3; 19.1 versions prior to 19.1R1-S4, 19.1R2; 19.2 versions prior to 19.2R1-S3, 19.2R2, This issue does not affect Junos OS releases prior to 17.4R1. This issue affects: Juniper Networks Junos OS Evolved 19.2-EVO versions prior to 19.2R2-EVO. CVE ID : CVE-2021-0250		
NULL Pointer Dereference	22-04-2021	5	A NULL Pointer Dereference vulnerability in the Captive Portal Content Delivery (CPCD) services daemon (cpd) of Juniper Networks Junos OS on MX Series with MS-PIC, MS-SPC3, MS-MIC or MS-MPC allows an attacker to send malformed HTTP packets to the device thereby causing a Denial of Service (DoS), crashing the Multiservices PIC Management Daemon (mcpmand) process thereby denying users the ability to login, while concurrently impacting other mcpmand services and traffic through the device. Continued receipt and processing of these malformed packets will create a sustained Denial of Service (DoS) condition. While the Services PIC is restarting, all PIC services will be bypassed until the Services PIC completes its boot process. An attacker sending these malformed	https://kb.juniper.net/JS_A11144	O-JUN-JUNO-040521/831

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>HTTP packets to the device who is not part of the Captive Portal experience is not able to exploit this issue. This issue is not applicable to MX RE-based CPCD platforms. This issue affects: Juniper Networks Junos OS on MX Series 17.3 version 17.3R1 and later versions prior to 17.4 versions 17.4R2-S9, 17.4R3-S2; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S3; 18.3 versions prior to 18.3R3-S1; 18.4 versions prior to 18.4R3; 19.1 versions prior to 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R2; 19.3 versions prior to 19.3R3. This issue does not affect: Juniper Networks Junos OS versions prior to 17.3R1.</p> <p>CVE ID : CVE-2021-0251</p>		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-04-2021	4.6	<p>NFX Series devices using Juniper Networks Junos OS are susceptible to a local code execution vulnerability thereby allowing an attacker to elevate their privileges via the Junos Device Management Daemon (JDMD) process. This issue affects Juniper Networks Junos OS on NFX Series: 18.1 version 18.1R1 and later versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to</p>	https://kb.juniper.net/JS_A11145	O-JUN-JUNO-040521/832

CVSS Scoring Scale	0-1	1-2	2-3	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-S5, 18.4R3-S4; 19.1 versions prior to 19.1R1-S3, 19.1R2; 19.2 versions prior to 19.2R1-S5, 19.2R2. This issue does not affect: Juniper Networks Junos OS versions prior to 18.1R1. This issue does not affect the JDMD as used by Junos Node Slicing such as External Servers use in conjunction with Junos Node Slicing and In-Chassis Junos Node Slicing on MX480, MX960, MX2008, MX2010, MX2020. CVE ID : CVE-2021-0252		
Improper Input Validation	22-04-2021	5	An Improper Input Validation vulnerability in the active-lease query portion in JDHCPD's DHCP Relay Agent of Juniper Networks Junos OS allows an attacker to cause a Denial of Service (DoS) by sending a crafted DHCP packet to the device thereby crashing the jdhcpd DHCP service. This is typically configured for Broadband Subscriber Sessions. Continued receipt and processing of this crafted packet will create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS: 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2-S1, 20.1R3; 20.2 versions prior to 20.2R3; 20.3 versions prior to 20.3R2. This issue	https://kb.juniper.net/JS_A11158 , https://www.juniper.net/documentation/us/en/software/junos/subscriber-mgmt-sessions/topics/ref/state-ment/active-leasequery-edit-forwarding-options.html	O-JUN-JUNO-040521/833

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			does not affect Junos OS Evolved. CVE ID : CVE-2021-0267		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2021	5.8	An Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting') weakness in J-web of Juniper Networks Junos OS leads to buffer overflows, segment faults, or other impacts, which allows an attacker to modify the integrity of the device and exfiltration information from the device without authentication. The weakness can be exploited to facilitate cross-site scripting (XSS), cookie manipulation (modifying session cookies, stealing cookies) and more. This weakness can also be exploited by directing a user to a seemingly legitimate link from the affected site. The attacker requires no special access or permissions to the device to carry out such attacks. This issue affects: Juniper Networks Junos OS: 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S3; 19.1 versions prior to 19.1R2-S2, 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R3; 19.4 versions prior	https://kb.juniper.net/JS_A11159	O-JUN-JUNO-040521/834

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to 19.4R1-S3, 19.4R2, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2. This issue does not affect Juniper Networks Junos OS versions prior to 18.1R1. CVE ID : CVE-2021-0268		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	4.3	On PTX Series and QFX10k Series devices with the "inline-jflow" feature enabled, a use after free weakness in the Packet Forwarding Engine (PFE) microkernel architecture of Juniper Networks Junos OS may allow an attacker to cause a Denial of Service (DoS) condition whereby one or more Flexible PIC Concentrators (FPCs) may restart. As this is a race condition situation this issue become more likely to be hit when network instability occurs, such as but not limited to BGP/IGP reconvergences, and/or further likely to occur when more active "traffic flows" are occurring through the device. When this issue occurs, it will cause one or more FPCs to restart unexpectedly. During FPC restarts core files will be generated. While the core file is generated traffic will be disrupted. Sustained receipt of large traffic flows and reconvergence-like situations may sustain the Denial of Service (DoS) situation. This issue affects:	https://kb.juniper.net/JS_A11161 , https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/inline-flow-monitoring-ptx.html	O-JUN-JUNO-040521/835

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Juniper Networks Junos OS: 18.1 version 18.1R2 and later versions prior to 18.1R3-S10 on PTX Series, QFX10K Series. CVE ID : CVE-2021-0270		
Allocation of Resources Without Limits or Throttling	22-04-2021	5	A vulnerability in the handling of internal resources necessary to bring up a large number of Layer 2 broadband remote access subscriber (BRAS) nodes in Juniper Networks Junos OS can cause the Access Node Control Protocol daemon (ANCPD) to crash and restart, leading to a Denial of Service (DoS) condition. Continued processing of spoofed subscriber nodes will create a sustained Denial of Service (DoS) condition. When the number of subscribers attempting to connect exceeds the configured maximum-discovery-table-entries value, the subscriber fails to map to an internal neighbor entry, causing the ANCPD process to crash. This issue affects Juniper Networks Junos OS: All versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R2-S13; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R3-S8; 19.1 versions prior to 19.1R3-S4;	https://kb.juniper.net/JS_A11119	O-JUN-JUNO-040521/836

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.2 versions prior to 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2; 20.3 versions prior to 20.3R2. CVE ID : CVE-2021-0224		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-04-2021	5	An improper restriction of operations within the bounds of a memory buffer vulnerability in Juniper Networks Junos OS J-Web on SRX Series devices allows an attacker to cause Denial of Service (DoS) by sending certain crafted HTTP packets. Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. When this issue occurs, web-management, NTP daemon (ntpd) and Layer 2 Control Protocol process (L2CPD) daemons might crash. This issue affects Juniper Networks Junos OS on SRX Series: 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R3-S2; 19.2 versions prior to 19.2R1-S5, 19.2R3; 19.3 versions prior to 19.3R3; 19.4 versions prior	https://kb.juniper.net/JS_A11122	O-JUN-JUNO-040521/837

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to 19.4R2-S1, 19.4R3; 20.1 versions prior to 20.1R1-S2, 20.1R2; CVE ID : CVE-2021-0227		
Improper Handling of Exceptional Conditions	22-04-2021	5	On Juniper Networks Junos OS platforms configured as DHCPv6 local server or DHCPv6 Relay Agent, Juniper Networks Dynamic Host Configuration Protocol Daemon (JDHCPD) process might crash with a core dump if a specific DHCPv6 packet is received, resulting in a restart of the daemon. The daemon automatically restarts without intervention, but continued receipt and processing of these specific packets will repeatedly crash the JDHCPD process and sustain the Denial of Service (DoS) condition. This issue only affects DHCPv6. DHCPv4 is not affected by this issue. This issue affects: Juniper Networks Junos OS 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S7; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R3-S1, 19.3R3-S2; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3;	https://kb.juniper.net/JS_A11168	O-JUN-JUNO-040521/838

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. CVE ID : CVE-2021-0241		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-04-2021	6.1	A vulnerability due to the improper handling of direct memory access (DMA) buffers on EX4300 switches on Juniper Networks Junos OS allows an attacker sending specific unicast frames to trigger a Denial of Service (DoS) condition by exhausting DMA buffers, causing the FPC to crash and the device to restart. The DMA buffer leak is seen when receiving these specific, valid unicast frames on an interface without Layer 2 Protocol Tunneling (L2PT) or dot1x configured. Interfaces with either L2PT or dot1x configured are not vulnerable to this issue. When this issue occurs, DMA buffer usage keeps increasing and the following error log messages may be observed: Apr 14 14:29:34.360 /kernel: pid 64476 (pfex_junos), uid 0: exited on signal 11 (core dumped) Apr 14 14:29:33.790 init: pfe-manager (PID 64476) terminated by signal number 11. Core dumped! The DMA buffers on the FPC can be monitored by the executing vty command	https://kb.juniper.net/JS_A11135	O-JUN-JUNO-040521/839

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			'show heap': ID Base Total(b) Free(b) Used(b) % Name -- ----- ----- 0 4a46000 268435456 238230496 30204960 11 Kernel 1 18a46000 67108864 17618536 49490328 73 Bcm_sdk 2 23737000 117440512 18414552 99025960 84 DMA buf <<<<< keeps increasing 3 2a737000 16777216 16777216 0 0 DMA desc This issue affects Juniper Networks Junos OS on the EX4300: 17.3 versions prior to 17.3R3- S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3- S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2- S7, 18.4R3-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S3, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2-S1, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. CVE ID : CVE-2021-0242		
N/A	22-04-2021	3.3	Improper Handling of Unexpected Data in the firewall policer of Juniper Networks Junos OS on	https://kb.juniper.net/JS_A11136	O-JUN-JUNO-040521/840

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>EX4300 switches allows matching traffic to exceed set policer limits, possibly leading to a limited Denial of Service (DoS) condition. When the firewall policer discard action fails on a Layer 2 port, it will allow traffic to pass even though it exceeds set policer limits. Traffic will not get discarded, and will be forwarded even though a policer discard action is configured. When the issue occurs, traffic is not discarded as desired, which can be observed by comparing the Input bytes with the Output bytes using the following command:</p> <pre> user@junos> monitor interface traffic Interface Link Input bytes (bps) Output bytes (bps) ge- 0/0/0 Up 37425422 (82616) 37425354 (82616) <<<< egress ge-0/0/1 Up 37425898 (82616) 37425354 (82616) <<<< ingress The expected output, with input and output counters differing, is shown below: Interface Link Input bytes (bps) Output bytes (bps) ge- 0/0/0 Up 342420570 (54600) 342422760 (54600) <<<< egress ge- 0/0/1 Up 517672120 (84000) 342420570 (54600) <<<< ingress This issue only affects IPv4 policing. IPv6 traffic and </pre>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>firewall policing actions are not affected by this issue. This issue affects Juniper Networks Junos OS on the EX4300: All versions prior to 17.3R3-S10; 17.4 versions prior to 17.4R3-S3; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S6; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S6; 19.1 versions prior to 19.1R3-S3; 19.2 versions prior to 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2.</p> <p>CVE ID : CVE-2021-0243</p>		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	4.3	<p>A signal handler race condition exists in the Layer 2 Address Learning Daemon (L2ALD) of Juniper Networks Junos OS due to the absence of a specific protection mechanism to avoid a race condition which may allow an attacker to bypass the storm-control feature on devices. This issue is a corner case and only occurs during specific actions taken by an administrator of a device under certain specific actions which triggers the event. The event occurs less frequently on devices which are not configured with Virtual</p>	https://kb.juniper.net/JS_A11137	O-JUN-JUNO-040521/841

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Chassis configurations, and more frequently on devices configured in Virtual Chassis configurations. This issue is not specific to any particular Junos OS platform. An Indicator of Compromise (IoC) may be seen by reviewing log files for the following error message seen by executing the following show statement: show log messages grep storm Result to look for: /kernel: GENCFG: op 58 (Storm Control Blob) failed; err 1 (Unknown) This issue affects: Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D49 on EX Series; 15.1 versions prior to 15.1R7-S6; 15.1X49 versions prior to 15.1X49-D191, 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3; 17.2 versions prior to 17.2R2-S8, 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S5; 18.2 versions prior to 18.2R2-S6, 18.2R3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R1-S5, 18.4R2; 19.1 versions prior to 19.1R1-S4, 19.1R2.		

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-0244		
Incorrect Authorization	22-04-2021	7.5	An improper authorization vulnerability in the Simple Network Management Protocol daemon (snmpd) service of Juniper Networks Junos OS leads an unauthenticated attacker being able to perform SNMP read actions, an Exposure of System Data to an Unauthorized Control Sphere, or write actions to OIDs that support write operations, against the device without authentication. This issue affects: Juniper Networks Junos OS: 17.2 version 17.2R1 and later versions; 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S12, 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S6, 19.2R2; 19.3 versions prior to 19.3R2. This issue does not affect Juniper Networks Junos OS versions prior to 17.2R1. CVE ID : CVE-2021-0260	https://kb.juniper.net/JS_A11151	O-JUN-JUNO-040521/842
Uncontrolled Resource Consumption	22-04-2021	5	An uncontrolled resource consumption vulnerability in Message Queue Telemetry Transport (MQTT) server of Juniper	https://kb.juniper.net/JS_A11124	O-JUN-JUNO-040521/843

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Networks Junos OS allows an attacker to cause MQTT server to crash and restart leading to a Denial of Service (DoS) by sending a stream of specific packets. A Juniper Extension Toolkit (JET) application designed with a listening port uses the Message Queue Telemetry Transport (MQTT) protocol to connect to a mosquitto broker that is running on Junos OS to subscribe for events. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS: 16.1R1 and later versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R2-S1, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2. This issue does not affect Juniper Networks</p>		

CVSS Scoring Scale	0-1	1-2	2-3	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 prior to 16.1R1. CVE ID : CVE-2021-0229								
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-04-2021	6.8	A path traversal vulnerability in the Juniper Networks SRX and vSRX Series may allow an authenticated J-web user to read sensitive system files. This issue affects Juniper Networks Junos OS on SRX and vSRX Series: 19.3 versions prior to 19.3R2-S6, 19.3R3-S1; 19.4 versions prior to 19.4R2-S4, 19.4R3; 20.1 versions prior to 20.1R1-S4, 20.1R2; 20.2 versions prior to 20.2R1-S3, 20.2R2; This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1. CVE ID : CVE-2021-0231	https://kb.juniper.net/JS_A11126	O-JUN-JUNO-040521/844						
Improper Check for Unusual or Exceptional Conditions	22-04-2021	6.8	Due to an improper check for unusual or exceptional conditions in Juniper Networks Junos OS and Junos OS Evolved the Routing Protocol Daemon (RPD) service, upon receipt of a specific matching BGP packet meeting a specific term in the flowspec configuration, crashes and restarts causing a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue affects only Multiprotocol BGP (MP-BGP) VPNv6 FlowSpec deployments.	https://kb.juniper.net/JS_A11131	O-JUN-JUNO-040521/845						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>This issue affects: Juniper Networks Junos OS: 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2.</p> <p>Juniper Networks Junos OS Evolved: All versions after 18.4R1-EVO prior to 20.3R2-EVO. This issue does not affect: Juniper Networks Junos OS versions prior to 18.4R1. Juniper Networks Junos OS Evolved versions prior to 18.4R1-EVO.</p> <p>CVE ID : CVE-2021-0236</p>		
Uncontrolled Resource Consumption	22-04-2021	2.1	<p>When a MX Series is configured as a Broadband Network Gateway (BNG) based on Layer 2 Tunneling Protocol (L2TP), executing certain CLI command may cause the system to run out of disk space, excessive disk usage may cause other complications. An administrator can use the following CLI command to monitor the available disk space: user@device> show system storage Filesystem Size Used Avail Capacity Mounted on</p>	https://kb.juniper.net/JS_A11133	O-JUN-JUNO-040521/846

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			/dev/gpt/junos 19G 18G 147M 99% /.mount <<<<< running out of space tmpfs 21G 16K 21G 0% /.mount/tmp tmpfs 5.3G 1.7M 5.3G 0% /.mount/mfs This issue affects Juniper Networks Junos OS on MX Series: 17.3R1 and later versions prior to 17.4R3-S5, 18.1 versions prior to 18.1R3-S13, 18.2 versions prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R3-S7; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2; 20.4 versions prior to 20.4R1-S1, 20.4R2; This issue does not affect Juniper Networks Junos OS versions prior to 17.3R1. CVE ID : CVE-2021-0238		
Improper Handling of Exceptional Conditions	22-04-2021	5	On Juniper Networks Junos OS platforms configured as DHCPv6 local server or DHCPv6 Relay Agent, the Juniper Networks Dynamic Host Configuration Protocol Daemon (JDHCPD) process might crash if a malformed DHCPv6 packet is received, resulting in a restart of the daemon. The daemon automatically restarts	https://kb.juniper.net/JS_A11168	O-JUN-JUNO-040521/847

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>without intervention, but continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue only affects DHCPv6. DHCPv4 is not affected by this issue. This issue affects Juniper Networks Junos OS: 17.3 versions prior to 17.3R3-S12; 17.4 versions prior to 17.4R3-S5; 18.1 versions prior to 18.1R3-S13; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S5; 18.4 versions prior to 18.4R1-S8, 18.4R3-S7; 19.1 versions prior to 19.1R3-S5; 19.2 versions prior to 19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2; 20.4 versions prior to 20.4R2.</p> <p>CVE ID : CVE-2021-0240</p>		
Use of Hard-coded Credentials	22-04-2021	7.2	<p>A Use of Hard-coded Credentials vulnerability in Juniper Networks Junos OS on Junos Fusion satellite devices allows an attacker who is local to the device to elevate their privileges and take control of the device. This issue affects: Juniper Networks Junos OS Junos Fusion Satellite Devices. 16.1 versions prior to 16.1R7-S7; 17.1 versions</p>	https://kb.juniper.net/JS_A11138	O-JUN-JUNO-040521/848

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>prior to 17.1R2-S12, 17.1R3-S2; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S10; 17.4 version 17.4R3 and later versions; 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, 18.3R2-S4, 18.3R3-S2; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3-S1; 19.1 versions prior to 19.1R1-S5, 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S4, 19.2R2; 19.3 versions prior to 19.3R2-S5, 19.3R3; 19.4 versions prior to 19.4R1-S1, 19.4R2; 20.1 versions prior to 20.1R1-S1, 20.1R2. This issue does not affected Junos OS releases prior to 16.1R1 or all 19.2R3 and 19.4R3 release versions.</p> <p>CVE ID : CVE-2021-0245</p>		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	6.8	<p>A Race Condition (Concurrent Execution using Shared Resource with Improper Synchronization) vulnerability in the firewall process (dfwd) of Juniper Networks Junos OS allows an attacker to bypass the firewall rule sets applied to the input loopback filter on any interfaces of a device. This issue is detectable by reviewing the PFE firewall rules, as well as the firewall counters and seeing if they</p>	https://kb.juniper.net/JS_A11140	O-JUN-JUNO-040521/849

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>are incrementing or not. For example: show firewall Filter:</p> <p><code>__default_bpdu_filter__</code></p> <p>Filter: FILTER-INET-01</p> <p>Counters: Name Bytes</p> <p>Packets output-match-inet</p> <p>0 0 <<<<< missing firewall packet count This issue affects: Juniper Networks Junos OS 14.1X53 versions prior to 14.1X53-D53 on QFX Series; 14.1 versions 14.1R1 and later versions prior to 15.1 versions prior to 15.1R7-S6 on QFX Series, PTX Series; 15.1X53 versions prior to 15.1X53-D593 on QFX Series; 16.1 versions prior to 16.1R7-S7 on QFX Series, PTX Series; 16.2 versions prior to 16.2R2-S11, 16.2R3 on QFX Series, PTX Series; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2 on QFX Series, PTX Series; 17.2 versions prior to 17.2R1-S9, 17.2R3-S3 on QFX Series, PTX Series; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7 on QFX Series, PTX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3 on QFX Series, PTX Series; 18.1 versions prior to 18.1R3-S9 on QFX Series, PTX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on QFX Series, PTX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1 on QFX Series, PTX Series; 18.4 versions prior to 18.4R1-S5,</p>		

CVSS Scoring Scale	0-1	1-2	2-3	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-S3, 18.4R2-S7, 18.4R3 on QFX Series, PTX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on QFX Series, PTX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on QFX Series, PTX Series. CVE ID : CVE-2021-0247		
Incorrect Calculation of Buffer Size	22-04-2021	7.5	A buffer size validation vulnerability in the overlayd service of Juniper Networks Junos OS may allow an unauthenticated remote attacker to send specially crafted packets to the device, triggering a partial Denial of Service (DoS) condition, or leading to remote code execution (RCE). Continued receipt and processing of these packets will sustain the partial DoS. The overlayd daemon handles Overlay OAM packets, such as ping and traceroute, sent to the overlay. The service runs as root by default and listens for UDP connections on port 4789. This issue results from improper buffer size validation, which can lead to a buffer overflow. Unauthenticated attackers can send specially crafted packets to trigger this vulnerability, resulting in possible remote code execution. overlayd runs by default in MX Series, ACX Series, and QFX Series platforms. The SRX Series	https://kb.juniper.net/JS_A11147	O-JUN-JUNO-040521/850

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>does not support VXLAN and is therefore not vulnerable to this issue. Other platforms are also vulnerable if a Virtual Extensible LAN (VXLAN) overlay network is configured. This issue affects Juniper Networks Junos OS: 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R2-S2, 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2-S1, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R2-S1, 20.2R3; 20.3 versions prior to 20.3R1-S1.</p> <p>CVE ID : CVE-2021-0254</p>		
Improper Privilege Management	22-04-2021	2.1	<p>A sensitive information disclosure vulnerability in the mosquito message broker of Juniper Networks Junos OS may allow a locally authenticated user with shell access the ability to read portions of sensitive files, such as the master.passwd file. Since</p>	https://kb.juniper.net/JS_A11175	O-JUN-JUNO-040521/851

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>mosquitto is shipped with setuid permissions enabled and is owned by the root user, this vulnerability may allow a local privileged user the ability to run mosquitto with root privileges and access sensitive information stored on the local filesystem. This issue affects Juniper Networks Junos OS: 17.3 versions prior to 17.3R3-S12, 17.4 versions prior to 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.3 versions prior to 18.3R3-S4; 19.1 versions prior to 19.1R3-S4; 19.3 versions prior to 19.3R3-S1, 19.3R3-S2; 19.4 versions prior to 19.4R2-S3; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R1-S3, 20.2R2, 20.2R3.</p> <p>CVE ID : CVE-2021-0256</p>		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	7.1	<p>A vulnerability in the forwarding of transit TCPv6 packets received on the Ethernet management interface of Juniper Networks Junos OS allows an attacker to trigger a kernel panic, leading to a Denial of Service (DoS). Continued receipt and processing of these transit packets will create a sustained Denial of Service (DoS) condition. This issue only occurs when TCPv6 packets are routed through the management interface. Other transit traffic, and</p>	https://kb.juniper.net/JS_A11149	O-JUN-JUNO-040521/852

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>traffic destined to the management interface, are unaffected by this vulnerability. This issue was introduced as part of a TCP Parallelization feature added in Junos OS 17.2, and affects systems with concurrent network stack enabled. This feature is enabled by default, but can be disabled (see WORKAROUND section below). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S9; 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.1 versions prior to 18.1R3-S11; 18.2 versions prior to 18.2R3-S5; 18.3 versions prior to 18.3R2-S4, 18.3R3-S3; 18.4 versions prior to 18.4R2-S5, 18.4R3-S4; 19.1 versions prior to 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S4, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2. This issue does not affect Juniper Networks Junos OS versions prior to 17.2R1.</p> <p>CVE ID : CVE-2021-0258</p>		
Improper Neutralization of Input During Web Page Generation ('Cross-site	22-04-2021	9.3	<p>A Cross-site Scripting (XSS) vulnerability in J-Web on Juniper Networks Junos OS allows an attacker to target another user's session thereby gaining access to the users session. The other</p>	https://kb.juniper.net/JS_A11166	O-JUN-JUNO-040521/853

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			<p>user session must be active for the attack to succeed. Once successful, the attacker has the same privileges as the user. If the user has root privileges, the attacker may be able to gain full control of the device. This issue affects: Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S15 on EX Series; 12.3X48 versions prior to 12.3X48-D95 on SRX Series; 15.1 versions prior to 15.1R7-S6 on EX Series; 15.1X49 versions prior to 15.1X49-D200 on SRX Series; 16.1 versions prior to 16.1R7-S7; 16.2 versions prior to 16.2R2-S11, 16.2R3; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S7; 17.4 versions prior to 17.4R2-S9, 17.4R3; 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3-S1; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3; 19.1 versions prior to 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S3, 19.2R2; 19.3 versions prior to 19.3R2.</p> <p>CVE ID : CVE-2021-0275</p>		
Uncontrolled Resource Consumption	22-04-2021	5	A vulnerability in Juniper Networks Junos OS running on the ACX5448 and	https://kb.juniper.net/JS_A11118	O-JUN-JUNO-040521/854

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>ACX710 platforms may cause BFD sessions to flap when a high rate of transit ARP packets are received. This, in turn, may impact routing protocols and network stability, leading to a Denial of Service (DoS) condition. When a high rate of transit ARP packets are exceptioned to the CPU and BFD flaps, the following log messages may be seen:</p> <p>bfdd[15864]: BFDD_STATE_UP_TO_DOWN: BFD Session 192.168.14.3 (IFL 232) state Up -> Down LD/RD(17/19) Up time:11:38:17 Local diag: CtlExpire Remote diag: None Reason: Detect Timer Expiry. bfdd[15864]: BFDD_TRAP_SHOP_STATE_DOWN: local discriminator: 17, new state: down, interface: irb.998, peer addr: 192.168.14.3 rpd[15839]: RPD_ISIS_ADJDOWN: IS-IS lost L2 adjacency to peer on irb.998, reason: BFD Session Down bfdd[15864]: BFDD_TRAP_SHOP_STATE_UP: local discriminator: 17, new state: up, interface: irb.998, peer addr: 192.168.14.3 This issue only affects the ACX5448 Series and ACX710 Series routers. No other products or platforms are affected by this vulnerability. This issue affects Juniper Networks</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Junos OS: 18.2 versions prior to 18.2R3-S8 on ACX5448; 18.3 versions prior to 18.3R3-S5 on ACX5448; 18.4 versions prior to 18.4R1-S6, 18.4R3-S7 on ACX5448; 19.1 versions prior to 19.1R3-S5 on ACX5448; 19.2 versions prior to 19.2R2, 19.2R3 on ACX5448; 19.3 versions prior to 19.3R3 on ACX5448; 19.4 versions prior to 19.4R3 on ACX5448; 20.1 versions prior to 20.1R2 on ACX5448; 20.2 versions prior to 20.2R2 on ACX5448 and ACX710.</p> <p>CVE ID : CVE-2021-0216</p>		
Improper Check for Unusual or Exceptional Conditions	22-04-2021	5	<p>An improper check for unusual or exceptional conditions vulnerability in Juniper Networks MX Series platforms with Trio-based MPC (Modular Port Concentrator) deployed in (Ethernet VPN) EVPN- (Virtual Extensible LAN) VXLAN configuration, may allow an attacker sending specific Layer 2 traffic to cause Distributed Denial of Service (DDoS) protection to trigger unexpectedly, resulting in traffic impact. Continued receipt and processing of this specific Layer 2 frames will sustain the Denial of Service (DoS) condition. An indication of compromise is to check DDOS LACP violations:</p>	https://kb.juniper.net/JS_A11123	O-JUN-JUNO-040521/855

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>user@device> show ddos-protection protocols statistics brief match lacp</p> <p>This issue only affects the MX Series platforms with Trio-based MPC. No other products or platforms are affected. This issue affects: Juniper Networks Junos OS on MX Series: 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R2-S8, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S2; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S1, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2;</p> <p>CVE ID : CVE-2021-0228</p>		
Uncontrolled Resource Consumption	22-04-2021	5	<p>On Juniper Networks Junos OS platforms with link aggregation (lag) configured, executing any operation that fetches Aggregated Ethernet (AE) interface statistics, including but not limited to SNMP GET requests, causes a slow kernel memory leak. If all the available memory</p>	https://kb.juniper.net/JS_A11125	O-JUN-JUNO-040521/856

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>is consumed, the traffic will be impacted and a reboot might be required. The following log can be seen if this issue happens. /kernel: rt_pfe_veto: Memory over consumed. Op 1 err 12, rtsm_id 0:-1, msg type 72 /kernel: rt_pfe_veto: free kmem_map memory = (20770816) curproc = kmd</p> <p>An administrator can use the following CLI command to monitor the status of memory consumption (ifstat bucket): user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 2588977 162708K - 19633958 <<<<</p> <p>user@device > show system virtual-memory no-forwarding match ifstat Type InUse MemUse HighUse Limit Requests Limit Limit Size(s) ifstat 3021629 189749K - 22914415 <<<< This issue does not affect the following platforms: Juniper Networks MX Series. Juniper Networks PTX1000-72Q, PTX3000, PTX5000, PTX10001, PTX10002-60C, PTX10003_160C, PTX10003_80C, PTX10003_81CD, PTX10004, PTX10008, PTX10016 Series. Juniper Networks EX9200 Series. Juniper Networks ACX710,</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>ACX6360 Series. Juniper Networks NFX Series. This issue affects Juniper Networks Junos OS: 17.1 versions 17.1R3 and above prior to 17.3R3-S11; 17.4 versions prior to 17.4R3-S5; 18.2 versions prior to 18.2R3-S7, 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2. This issue does not affect Juniper Networks Junos OS prior to 17.1R3.</p> <p>CVE ID : CVE-2021-0230</p>		
N/A	22-04-2021	5	<p>On Juniper Networks EX4300-MP Series, EX4600 Series, EX4650 Series, QFX5K Series deployed as a Virtual Chassis with a specific Layer 2 circuit configuration, Packet Forwarding Engine manager (FXPC) process may crash and restart upon receipt of specific layer 2 frames. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks</p>	https://kb.juniper.net/JS_A11132	O-JUN-JUNO-040521/857

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Junos OS on EX4300-MP Series, EX4600 Series, EX4650 Series, QFX5K Series 15.1 versions prior to 15.1R7-S9; 17.3 versions prior to 17.3R3-S11; 17.4 versions prior to 17.4R2-S13, 17.4R3-S4, 17.4R3-S5; 18.2 versions prior to 18.2R3-S8; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7, 18.4R3-S6; 19.1 versions prior to 19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S1; 19.3 versions prior to 19.3R3-S1; 19.4 versions prior to 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S2, 20.3R2;</p> <p>CVE ID : CVE-2021-0237</p>		
Incorrect Default Permissions	22-04-2021	4.6	<p>On SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3, devices using tenant services on Juniper Networks Junos OS, due to incorrect default permissions assigned to tenant system administrators a tenant system administrator may inadvertently send their network traffic to one or more tenants while concurrently modifying the overall device system traffic management, affecting all tenants and the service provider. Further, a tenant</p>	https://kb.juniper.net/JS_A11139	O-JUN-JUNO-040521/858

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
			<p>may inadvertently receive traffic from another tenant. This issue affects: Juniper Networks Junos OS 18.3 version 18.3R1 and later versions on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2; 18.3 versions prior to 18.3R3 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2; 18.4 versions prior to 18.4R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3; 19.1 versions prior to 19.1R2 on SRX1500, SRX4100, SRX4200, SRX4600, SRX5000 Series with SPC2/SPC3. This issue does not affect: Juniper Networks Junos OS versions prior to 18.3R1.</p> <p>CVE ID : CVE-2021-0246</p>		
Use of Hard-coded Credentials	22-04-2021	7.5	<p>This issue is not applicable to NFX NextGen Software. On NFX Series devices the use of Hard-coded Credentials in Juniper Networks Junos OS allows an attacker to take over any instance of an NFX deployment. This issue is only exploitable through administrative interfaces. This issue affects: Juniper Networks Junos OS versions prior to 19.1R1 on NFX Series. No other platforms besides NFX Series devices</p>	https://kb.juniper.net/JS_A11141	O-JUN-JUNO-040521/859

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			are affected. CVE ID : CVE-2021-0248		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-04-2021	4.6	NFX Series devices using Juniper Networks Junos OS are susceptible to a local command execution vulnerability thereby allowing an attacker to elevate their privileges via the Junos Device Management Daemon (JDMD) process. This issue affects Juniper Networks Junos OS on NFX Series 17.2 version 17.2R1 and later versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S5, 18.4R3-S5; 19.1 versions prior to 19.1R1-S3; 19.2 version 19.1R2 and later versions prior to 19.2R3; 19.3 versions prior to 19.3R3; 19.4 versions prior to 19.4R2-S2. 19.4 versions 19.4R3 and above. This issue does not affect Juniper Networks Junos OS versions prior to 17.2R1. This issue does not affect the JDMD as used by Junos Node Slicing such as External Servers use in conjunction with Junos Node Slicing and In-Chassis Junos Node Slicing on MX480, MX960, MX2008, MX2010, MX2020. CVE ID : CVE-2021-0253	https://kb.juniper.net/JS_A11146	O-JUN-JUNO-040521/860
Improper Privilege Management	22-04-2021	7.2	A local privilege escalation vulnerability in ethtraceroute of Juniper Networks Junos OS may allow a locally	https://kb.juniper.net/JS_A11175	O-JUN-JUNO-040521/861

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>authenticated user with shell access to escalate privileges and write to the local filesystem as root. ethtraceroute is shipped with setuid permissions enabled and is owned by the root user, allowing local users to run ethtraceroute with root privileges. This issue affects Juniper Networks Junos OS: 15.1X49 versions prior to 15.1X49-D240; 17.3 versions prior to 17.3R3-S11, 17.4 versions prior to 17.4R3-S4; 18.1 versions prior to 18.1R3-S12; 18.2 versions prior to 18.2R3-S7; 18.3 versions prior to 18.3R3-S4; 18.4 versions prior to 18.4R2-S7; 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3-S4; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2-S1, 20.2R3; 20.3 versions prior to 20.3R1-S1.</p> <p>CVE ID : CVE-2021-0255</p>		
Improper Handling of Exceptional Conditions	22-04-2021	5	<p>A vulnerability in the processing of traffic matching a firewall filter containing a syslog action in Juniper Networks Junos OS on MX Series with MPC10/MPC11 cards installed, PTX10003 and PTX10008 Series devices, will cause the line card to crash and restart, creating a</p>	<p>https://kb.juniper.net/JS_A11155, https://kb.juniper.net/TS_B17931</p>	O-JUN-JUNO-040521/862

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Denial of Service (DoS). Continued receipt and processing of packets matching the firewall filter can create a sustained Denial of Service (DoS) condition. When traffic hits the firewall filter, configured on lo0 or any physical interface on the line card, containing a term with a syslog action (e.g. 'term <name> then syslog'), the affected line card will crash and restart, impacting traffic processing through the ports of the line card. This issue only affects MX Series routers with MPC10 or MPC11 line cards, and PTX10003 or PTX10008 Series packet transport routers. No other platforms or models of line cards are affected by this issue. Note: This issue has also been identified and described in technical service bulletin TSB17931 (login required). This issue affects: Juniper Networks Junos OS on MX Series: 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2. Juniper Networks Junos OS Evolved on PTX10003, PTX10008: All versions prior to 20.4R2-EVO. This issue does not</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affect Juniper Networks Junos OS versions prior to 19.3R1. CVE ID : CVE-2021-0264		
Use of Hard-coded Credentials	22-04-2021	7.5	The use of multiple hard-coded cryptographic keys in cSRX Series software in Juniper Networks Junos OS allows an attacker to take control of any instance of a cSRX deployment through device management services. This issue affects: Juniper Networks Junos OS on cSRX Series: All versions prior to 20.2R3; 20.3 versions prior to 20.3R2; 20.4 versions prior to 20.4R2. CVE ID : CVE-2021-0266	https://kb.juniper.net/JS_A11157	O-JUN-JUNO-040521/863
Double Free	22-04-2021	5	A Double Free vulnerability in the software forwarding interface daemon (sfid) process of Juniper Networks Junos OS allows an adjacently-connected attacker to cause a Denial of Service (DoS) by sending a crafted ARP packet to the device. Continued receipt and processing of the crafted ARP packets will create a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS on EX2200-C Series, EX3200 Series, EX3300 Series, EX4200 Series, EX4500 Series, EX4550 Series, EX6210 Series, EX8208 Series, EX8216 Series. 12.3 versions prior to 12.3R12-	https://kb.juniper.net/JS_A11162	O-JUN-JUNO-040521/864

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S17; 15.1 versions prior to 15.1R7-S8. This issue only affects the listed Marvell-chipset based EX Series devices. No other products or platforms are affected. CVE ID : CVE-2021-0271		
junos_os_evolved					
N/A	22-04-2021	5	In segment routing traffic engineering (SRTE) environments where the BGP Monitoring Protocol (BMP) feature is enable, a vulnerability in the Routing Protocol Daemon (RPD) process of Juniper Networks Junos OS allows an attacker to send a specific crafted BGP update message causing the RPD service to core, creating a Denial of Service (DoS) Condition. Continued receipt and processing of this update message will create a sustained Denial of Service (DoS) condition. This issue affects IPv4 and IPv6 environments. This issue affects: Juniper Networks Junos OS 17.4 versions 17.4R1 and above prior to 17.4R2-S6, 17.4R3; 18.1 versions prior to 18.1R3-S7; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R1-S5, 18.4R2-S3, 18.4R3; 19.1 versions prior to 19.1R1-S4, 19.1R2; 19.2 versions prior to 19.2R1-S3,	https://kb.juniper.net/JS_A11143	O-JUN-JUNO-040521/865

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.2R2, This issue does not affect Junos OS releases prior to 17.4R1. This issue affects: Juniper Networks Junos OS Evolved 19.2-EVO versions prior to 19.2R2-EVO. CVE ID : CVE-2021-0250		
Improper Check for Unusual or Exceptional Conditions	22-04-2021	5	An Improper Check for Unusual or Exceptional Conditions in Juniper Networks Junos OS Evolved may cause the stateless firewall filter configuration which uses the action 'policer' in certain combinations with other options to not take effect. An administrator can use the following CLI command to see the failures with filter configuration: user@device> show log kfirewall-agent.log match ERROR Jul 23 14:16:03 ERROR: filter not supported This issue affects Juniper Networks Junos OS Evolved: Versions 19.1R1-EVO and above prior to 20.3R1-S2-EVO, 20.3R2-EVO. This issue does not affect Juniper Networks Junos OS. CVE ID : CVE-2021-0225	https://kb.juniper.net/JS_A11120	O-JUN-JUNO-040521/866
Improper Initialization	22-04-2021	5	On Juniper Networks Junos OS Evolved devices, receipt of a specific IPv6 packet may cause an established IPv6 BGP session to terminate, creating a Denial of Service (DoS) condition. Continued receipt and processing of this packet	https://kb.juniper.net/JS_A11121	O-JUN-JUNO-040521/867

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			will create a sustained Denial of Service (DoS) condition. This issue does not affect IPv4 BGP sessions. This issue affects IBGP or EBGP peer sessions with IPv6. This issue affects: Juniper Networks Junos OS Evolved: 19.4 versions prior to 19.4R2-S3-EVO; 20.1 versions prior to 20.1R2-S3-EVO; 20.2 versions prior to 20.2R2-S1-EVO; 20.3 versions prior to 20.3R2-EVO. This issue does not affect Juniper Networks Junos OS releases. CVE ID : CVE-2021-0226		
Improper Check for Unusual or Exceptional Conditions	22-04-2021	6.8	Due to an improper check for unusual or exceptional conditions in Juniper Networks Junos OS and Junos OS Evolved the Routing Protocol Daemon (RPD) service, upon receipt of a specific matching BGP packet meeting a specific term in the flowspec configuration, crashes and restarts causing a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue affects only Multiprotocol BGP (MP-BGP) VPNv6 FlowSpec deployments. This issue affects: Juniper Networks Junos OS: 18.4 versions prior to 18.4R1-S8, 18.4R2-S7, 18.4R3-S7; 19.1 versions prior to 19.1R2-S2,	https://kb.juniper.net/JS_A11131	O-JUN-JUNO-040521/868

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>19.1R3-S4; 19.2 versions prior to 19.2R1-S6, 19.2R3-S2; 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R2-S4, 19.4R3-S1; 20.1 versions prior to 20.1R2, 20.1R3; 20.2 versions prior to 20.2R2, 20.2R3; 20.3 versions prior to 20.3R1-S1, 20.3R2.</p> <p>Juniper Networks Junos OS Evolved: All versions after 18.4R1-EVO prior to 20.3R2-EVO. This issue does not affect: Juniper Networks Junos OS versions prior to 18.4R1. Juniper Networks Junos OS Evolved versions prior to 18.4R1-EVO.</p> <p>CVE ID : CVE-2021-0236</p>		
Improper Check for Unusual or Exceptional Conditions	22-04-2021	6.1	<p>In Juniper Networks Junos OS Evolved, receipt of a stream of specific genuine Layer 2 frames may cause the Advanced Forwarding Toolkit (AFT) manager process (Evo-aftmand), responsible for handling Route, Class-of-Service (CoS), Firewall operations within the packet forwarding engine (PFE) to crash and restart, leading to a Denial of Service (DoS) condition. By continuously sending this specific stream of genuine Layer 2 frames, an attacker can repeatedly crash the PFE, causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS</p>	https://kb.juniper.net/JS_A11134	O-JUN-JUNO-040521/869

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Evolved: All versions prior to 20.4R1-EVO. This issue does not affect Junos OS versions.</p> <p>CVE ID : CVE-2021-0239</p>		
Improper Handling of Exceptional Conditions	22-04-2021	5	<p>A vulnerability in the processing of traffic matching a firewall filter containing a syslog action in Juniper Networks Junos OS on MX Series with MPC10/MPC11 cards installed, PTX10003 and PTX10008 Series devices, will cause the line card to crash and restart, creating a Denial of Service (DoS). Continued receipt and processing of packets matching the firewall filter can create a sustained Denial of Service (DoS) condition. When traffic hits the firewall filter, configured on lo0 or any physical interface on the line card, containing a term with a syslog action (e.g. 'term <name> then syslog'), the affected line card will crash and restart, impacting traffic processing through the ports of the line card. This issue only affects MX Series routers with MPC10 or MPC11 line cards, and PTX10003 or PTX10008 Series packet transport routers. No other platforms or models of line cards are affected by this issue. Note: This issue has also been identified and described in</p>	<p>https://kb.juniper.net/JS_A11155, https://kb.juniper.net/TS_B17931</p>	O-JUN-JUNO-040521/870

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			technical service bulletin TSB17931 (login required). This issue affects: Juniper Networks Junos OS on MX Series: 19.3 versions prior to 19.3R3-S2; 19.4 versions prior to 19.4R3-S2; 20.1 versions prior to 20.1R3; 20.2 versions prior to 20.2R2-S2, 20.2R3; 20.3 versions prior to 20.3R3; 20.4 versions prior to 20.4R2. Juniper Networks Junos OS Evolved on PTX10003, PTX10008: All versions prior to 20.4R2-EVO. This issue does not affect Juniper Networks Junos OS versions prior to 19.3R1. CVE ID : CVE-2021-0264							
linux										
linux_kernel										
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-04-2021	6.9	A race condition in Linux kernel SCTP sockets (net/sctp/socket.c) before 5.12-rc8 can lead to kernel privilege escalation from the context of a network service or an unprivileged process. If sctp_destroy_sock is called without sock_net(sk)->sctp.addr_wq_lock then an element is removed from the auto_asconf_splist list without any proper locking. This can be exploited by an attacker with network service privileges to escalate to root or from the context of an unprivileged user directly if a	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=b166a20b07382b8bc1dcee2a448715c9c2c81b5b , https://www.openwall.com/lists/oss-security/2021/04/18/2	O-LIN-LINU-040521/871					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BPF_CGROUP_INET_SOCK_CREATE is attached which denies creation of some SCTP socket. CVE ID : CVE-2021-23133		
N/A	26-04-2021	6.4	IBM Spectrum Protect Plus 10.1.0 through 10.1.7 uses Cross-Origin Resource Sharing (CORS) which could allow an attacker to carry out privileged actions and retrieve sensitive information as the domain name is not being limited to only trusted domains. IBM X-Force ID: 196344. CVE ID : CVE-2021-20432	https://exchange.xforce.ibmcloud.com/vulnerabilities/196344 , https://www.ibm.com/support/pages/node/6445733	O-LIN-LINU-040521/872
Out-of-bounds Write	30-04-2021	4.6	IBM Informix Dynamic Server 14.10 is vulnerable to a stack based buffer overflow, caused by improper bounds checking. A local privileged user could overflow a buffer and execute arbitrary code on the system or cause a denial of service condition. IBM X-Force ID: 198366. CVE ID : CVE-2021-20515	https://exchange.xforce.ibmcloud.com/vulnerabilities/198366 , https://www.ibm.com/support/pages/node/6448568	O-LIN-LINU-040521/873
Out-of-bounds Read	19-04-2021	5.6	An out-of-bounds (OOB) memory access flaw was found in fs/f2fs/node.c in the f2fs module in the Linux kernel in versions before 5.12.0-rc4. A bounds check failure allows a local attacker to gain access to out-of-bounds memory leading to a system crash or a leak of internal kernel information. The highest threat from this	https://www.mail-archive.com/linux-kernel@vger.kernel.org/msg2520013.html , https://www.openwall.com/lists/oss-security/202	O-LIN-LINU-040521/874

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			vulnerability is to system availability. CVE ID : CVE-2021-3506	1/03/28/2							
Inadequate Encryption Strength	26-04-2021	5	IBM Spectrum Protect Plus 10.1.0 through 10.1.7 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 200258. CVE ID : CVE-2021-29694	https://exchange.xforce.ibmcloud.com/vulnerabilities/200258 , https://www.ibm.com/support/pages/node/6445735	O-LIN-LINU-040521/875						
Out-of-bounds Read	20-04-2021	2.1	An issue was discovered in the Linux kernel through 5.11.x. kernel/bpf/verifier.c performs undesirable out-of-bounds speculation on pointer arithmetic, leading to side-channel attacks that defeat Spectre mitigations and obtain sensitive information from kernel memory. Specifically, for sequences of pointer arithmetic operations, the pointer modification performed by the first operation is not correctly accounted for when restricting subsequent operations. CVE ID : CVE-2021-29155	https://www.kernel.org , https://www.openwall.com/lists/oss-security/2021/04/18/4	O-LIN-LINU-040521/876						
microsoft											
windows											
Uncontrolled Search Path Element	19-04-2021	9.3	Adobe Robohelp version 2020.0.3 (and earlier) is affected by an uncontrolled search path element vulnerability that could lead to privilege escalation. An	https://helpx.adobe.com/security/products/robohelp/apsb21	O-MIC-WIND-040521/877						
CVSS Scoring Scale		0-1	1-2	2-3	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 with permissions to write to the file system could leverage this vulnerability to escalate privileges. CVE ID : CVE-2021-21070	-20.html	
N/A	20-04-2021	4.6	NVIDIA GeForce Experience, all versions prior to 3.22, contains a vulnerability in GameStream plugins where log files are created using NT/System level permissions, which may lead to code execution, denial of service, or local privilege escalation. CVE ID : CVE-2021-1079	https://nvidia.custhelp.com/app/answers/detail/a_id/5184	O-MIC-WIND-040521/878
Insertion of Sensitive Information into Log File	26-04-2021	2.1	IBM Spectrum Protect Plus File Systems Agent 10.1.6 and 10.1.7 stores potentially sensitive information in log files that could be read by a local user. IBM X-Force ID: 198836. CVE ID : CVE-2021-20536	https://www.ibm.com/support/pages/node/6445739 , https://exchange.xforce.ibmcloud.com/vulnerabilities/198836	O-MIC-WIND-040521/879
Out-of-bounds Write	30-04-2021	4.6	IBM Informix Dynamic Server 14.10 is vulnerable to a stack based buffer overflow, caused by improper bounds checking. A local privileged user could overflow a buffer and execute arbitrary code on the system or cause a denial of service condition. IBM X-Force ID: 198366. CVE ID : CVE-2021-20515	https://exchange.xforce.ibmcloud.com/vulnerabilities/198366 , https://www.ibm.com/support/pages/node/6448568	O-MIC-WIND-040521/880

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
Out-of-bounds Write	30-04-2021	6.8	Heap buffer overflow in ANGLE in Google Chrome on Windows prior to 90.0.4430.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-21233	https://crbug.com/1182937 , https://chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop_26.html	O-MIC-WIND-040521/881						
Incorrect Default Permissions	26-04-2021	7.2	IBM Spectrum Protect Client 8.1.0.0 through 8.1.11.0 could allow a local user to escalate their privileges to take full control of the system due to insecure directory permissions. IBM X-Force ID: 198811. CVE ID : CVE-2021-20532	https://www.ibm.com/support/pages/node/6445503 , https://exchange.xforce.ibmcloud.com/vulnerabilities/198811	O-MIC-WIND-040521/882						
nec											
aterm_wg2600hs_firmware											
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-04-2021	10	Aterm WG2600HS firmware Ver1.5.1 and earlier allows an attacker to execute arbitrary OS commands via unspecified vectors. CVE ID : CVE-2021-20711	https://jpn.nec.com/security-info/secinfo/nv21-010.html	O-NEC-ATER-040521/883						
oracle											
legal_entity_configurator											
N/A	22-04-2021	5.5	Vulnerability in the Oracle Legal Entity Configurator product of Oracle E-Business Suite (component: Create Contracts). Supported versions that are	https://www.oracle.com/security-alerts/cpuapr2021.html	O-ORA-LEGA-040521/884						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>affected are 12.1.1-12.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Legal Entity Configurator. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Legal Entity Configurator accessible data as well as unauthorized access to critical data or complete access to all Oracle Legal Entity Configurator accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).</p> <p>CVE ID : CVE-2021-2273</p>		
solaris					
N/A	22-04-2021	4.6	<p>Vulnerability in the Oracle Solaris product of Oracle Systems (component: Common Desktop Environment). The supported version that is affected is 10. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in takeover of Oracle Solaris.</p>	https://www.oracle.com/security-alerts/cpuapr2021.html	O-ORA-SOLA-040521/885

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). CVE ID : CVE-2021-2167								
N/A	22-04-2021	3.6	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Kernel). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris as well as unauthorized update, insert or delete access to some of Oracle Solaris accessible data. Note: This vulnerability applies to Oracle Solaris on SPARC systems only. CVSS 3.1 Base Score 6.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H). CVE ID : CVE-2021-2192	https://www.oracle.com/security-alerts/cpuapr2021.html	O-ORA-SOLA-040521/886						
Out-of-bounds Write	30-04-2021	4.6	IBM Informix Dynamic Server 14.10 is vulnerable to a stack based buffer overflow, caused by improper bounds checking.	https://exchange.xforce.ibmcloud.com/vulnerabilities/19836	O-ORA-SOLA-040521/887						
CVSS Scoring Scale		0-1	1-2	2-3	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 local privileged user could overflow a buffer and execute arbitrary code on the system or cause a denial of service condition. IBM X-Force ID: 198366. CVE ID : CVE-2021-20515	6, https://www.ibm.com/support/pages/node/6448568	
zfs_storage_appliance					
N/A	22-04-2021	1.2	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: Installation). The supported version that is affected is 8.8. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle ZFS Storage Appliance Kit executes to compromise Oracle ZFS Storage Appliance Kit. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle ZFS Storage Appliance Kit accessible data. CVSS 3.1 Base Score 1.8 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:N). CVE ID : CVE-2021-2147	https://www.oracle.com/security-alerts/cpuapr2021.html	O-ORA-ZFS_-040521/888
N/A	22-04-2021	1.9	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: Core). The supported version that is	https://www.oracle.com/security-alerts/cpuapr2021.html	O-ORA-ZFS_-040521/889

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			affected is 8.8. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle ZFS Storage Appliance Kit executes to compromise Oracle ZFS Storage Appliance Kit. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle ZFS Storage Appliance Kit accessible data. CVSS 3.1 Base Score 2.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N). CVE ID : CVE-2021-2149							
paloaltonetworks										
pan-os										
Insertion of Sensitive Information into Log File	20-04-2021	2.1	An information exposure through log file vulnerability exists in Palo Alto Networks PAN-OS software where secrets in PAN-OS XML API requests are logged in cleartext to the web server logs when the API is used incorrectly. This vulnerability applies only to PAN-OS appliances that are configured to use the PAN-OS XML API and exists only when a client includes a duplicate API parameter in API requests. Logged information includes the cleartext username, password, and API key of the administrator making the PAN-OS XML	https://security.paloaltonetworks.com/CVE-2021-3036	O-PAL-PAN--040521/890					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			API request. CVE ID : CVE-2021-3036		
Insertion of Sensitive Information into Log File	20-04-2021	2.1	An information exposure through log file vulnerability exists in Palo Alto Networks PAN-OS software where the connection details for a scheduled configuration export are logged in system logs. Logged information includes the cleartext username, password, and IP address used to export the PAN-OS configuration to the destination server. CVE ID : CVE-2021-3037	https://security.paloaltonetworks.com/CVE-2021-3037	O-PAL-PAN--040521/891
redhat					
enterprise_linux					
Incorrect Privilege Assignment	19-04-2021	4.9	A flaw was found in cifs-utils in versions before 6.13. A user when mounting a krb5 CIFS file system from within a container can use Kerberos credentials of the host. The highest threat from this vulnerability is to data confidentiality and integrity. CVE ID : CVE-2021-20208	https://bugzilla.samba.org/show_bug.cgi?id=14651	O-RED-ENTE-040521/892
Use After Free	19-04-2021	6.8	GStreamer before 1.18.4 might access already-freed memory in error code paths when demuxing certain malformed Matroska files. CVE ID : CVE-2021-3497	https://gstreamer.freedesktop.org/security/sa-2021-0002.html , https://bugzilla.redhat.com/show_bug.cgi?id=1945339	O-RED-ENTE-040521/893

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insufficient Entropy	19-04-2021	2.1	A flaw was found in libtpms in versions before 0.8.0. The TPM 2 implementation returns 2048 bit keys with ~1984 bit strength due to a bug in the TCG specification. The bug is in the key creation algorithm in RsaAdjustPrimeCandidate(), which is called before the prime number check. The highest threat from this vulnerability is to data confidentiality. CVE ID : CVE-2021-3505	https://bugzilla.redhat.com/show_bug.cgi?id=1950046 , https://github.com/stefanberger/libtpms/issues/183	O-RED-ENTE-040521/894
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-04-2021	6.8	GStreamer before 1.18.4 might cause heap corruption when parsing certain malformed Matroska files. CVE ID : CVE-2021-3498	https://gstreamer.freedesktop.org/security/sa-2021-0003.html , https://bugzilla.redhat.com/show_bug.cgi?id=1945342	O-RED-ENTE-040521/895
siemens					
nucleus_rtos					
Use of Insufficiently Random Values	22-04-2021	5	A vulnerability has been identified in Nucleus 4 (All versions < V4.1.0), Nucleus NET (All versions), Nucleus RTOS (versions including affected DNS modules), Nucleus ReadyStart (All versions < V2017.02.3), Nucleus Source Code (versions including affected DNS modules), SIMOTICS CONNECT 400 (All versions < V0.5.0.0), SIMOTICS CONNECT 400 (All versions	https://certportal.siemens.com/productcert/pdf/ssa-705111.pdf , https://certportal.siemens.com/productcert/pdf/ssa-669158.pdf	O-SIE-NUCL-040521/896

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			>= V0.5.0.0), VSTAR (versions including affected DNS modules). The DNS client does not properly randomize DNS transaction IDs. That could allow an attacker to poison the DNS cache or spoof DNS resolving. CVE ID : CVE-2021-25677		
Use of Insufficiently Random Values	22-04-2021	5	A vulnerability has been identified in Nucleus NET (All versions), Nucleus RTOS (versions including affected DNS modules), Nucleus ReadyStart (All versions < V2013.08), Nucleus Source Code (versions including affected DNS modules), VSTAR (versions including affected DNS modules). The DNS client does not properly randomize UDP port numbers of DNS requests. That could allow an attacker to poison the DNS cache or spoof DNS resolving. CVE ID : CVE-2021-27393	https://certportal.siemens.com/productcert/pdf/ssa-201384.pdf	O-SIE-NUCL-040521/897
scalance_x200-4p_irt_firmware					
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant)	https://certportal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/898

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect		

CVSS Scoring Scale	0-1	1-2	2-3	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 of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code. CVE ID : CVE-2021-25668		
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions),	https://certportal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/899

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution.</p> <p>CVE ID : CVE-2021-25669</p>		
scalance_x201-3p_irt_firmware					
Out-of-bounds Write	22-04-2021	7.5	<p>A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT</p>	<p>https://certportal.siemens.com/productcert/pdf/ssa-187092.pdf</p>	O-SIE-SCAL-040521/900

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204- 2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204- 2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206- 1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212- 2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202- 2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver		

CVSS Scoring Scale	0-1	1-2	2-3	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 result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code. CVE ID : CVE-2021-25668		
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/901

CVSS Scoring Scale	0-1	1-2	2-3	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), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution. CVE ID : CVE-2021-25669		
scalance_x201-3p_irt_pro_firmware					
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/902

CVSS Scoring Scale	0-1	1-2	2-3	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 < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker		

CVSS Scoring Scale	0-1	1-2	2-3	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 leverage this to cause denial-of-service on the device and potentially remotely execute code. CVE ID : CVE-2021-25668		
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/903

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution.</p> <p>CVE ID : CVE-2021-25669</p>		

scalance_x202-2_irt_firmware

Out-of-bounds Write	22-04-2021	7.5	<p>A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO</p>	<p>https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf</p>	O-SIE-SCAL-040521/904
---------------------	------------	-----	--	--	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device and potentially remotely execute code. CVE ID : CVE-2021-25668		
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/905

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution. CVE ID : CVE-2021-25669		

scalance_x202-2p_irt_pro_firmware

Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl.	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/906
---------------------	------------	-----	---	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code.		

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-25668								
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/907						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution.</p> <p>CVE ID : CVE-2021-25669</p>		
scalance_x204_irt_firmware					
Out-of-bounds Write	22-04-2021	7.5	<p>A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions),</p>	<p>https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf</p>	O-SIE-SCAL-040521/908

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code.</p> <p>CVE ID : CVE-2021-25668</p>		
Out-of-	22-04-2021	7.5	A vulnerability has been	https://cert-	O-SIE-SCAL-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204	portal.siemens.com/productcert/pdf/ssa-187092.pdf	040521/909

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution. CVE ID : CVE-2021-25669		

scalance_x204_irt_pro_firmware

Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All	https://certportal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/910
---------------------	------------	-----	---	---	-----------------------

CVSS Scoring Scale	0-1	1-2	2-3	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), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code. CVE ID : CVE-2021-25668		
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions <	https://cert-portal.siemens.com/prod	O-SIE-SCAL-040521/911

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions <	uctcert/pdf/ssa-187092.pdf	

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution. CVE ID : CVE-2021-25669		

scalance_x204-2_firmware

Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/912
---------------------	------------	-----	---	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code.</p> <p>CVE ID : CVE-2021-25668</p>		
Out-of-bounds Write	22-04-2021	7.5	<p>A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1),</p>	https://certportal.siemens.com/productcert/pdf/ssa-	O-SIE-SCAL-040521/913

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant)	187092.pdf	

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution. CVE ID : CVE-2021-25669		

scalance_x204-2fm_firmware

Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/914
---------------------	------------	-----	--	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code.</p> <p>CVE ID : CVE-2021-25668</p>		
Out-of-bounds Write	22-04-2021	7.5	<p>A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1),</p>	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/915

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All		

CVSS Scoring Scale	0-1	1-2	2-3	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 < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution. CVE ID : CVE-2021-25669		
scalance_x204-2ld_firmware					
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions),	https://certportal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/916

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code.</p> <p>CVE ID : CVE-2021-25668</p>		
Out-of-bounds Write	22-04-2021	7.5	<p>A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1),</p>	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/917

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All		

CVSS Scoring Scale	0-1	1-2	2-3	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), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution. CVE ID : CVE-2021-25669		

scalance_x204-2ld_ts_firmware

Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All	https://certportal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/918
---------------------	------------	-----	---	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code. CVE ID : CVE-2021-25668		
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant)	https://certportal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/919

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect		

CVSS Scoring Scale	0-1	1-2	2-3	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 of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution. CVE ID : CVE-2021-25669		
scalance_x204-2ts_firmware					
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/920

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code.</p> <p>CVE ID : CVE-2021-25668</p>		
Out-of-bounds Write	22-04-2021	7.5	<p>A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT</p>	<p>https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf</p>	O-SIE-SCAL-040521/921

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204- 2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204- 2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206- 1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212- 2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202- 2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server		

CVSS Scoring Scale	0-1	1-2	2-3	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 write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution. CVE ID : CVE-2021-25669		
scalance_x206-1_firmware					
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/922

CVSS Scoring Scale	0-1	1-2	2-3	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), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code. CVE ID : CVE-2021-25668		
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All	https://certportal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/923

CVSS Scoring Scale	0-1	1-2	2-3	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 < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leverage this to denial-of-service of the device or remote code execution. CVE ID : CVE-2021-25669		
scalance_x206-1ld_firmware					
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions),	https://certportal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/924

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code.</p> <p>CVE ID : CVE-2021-25668</p>		
Out-of-bounds Write	22-04-2021	7.5	<p>A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO</p>	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/925

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote code execution. CVE ID : CVE-2021-25669		
scalance_x208_firmware					
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/926

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>(All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code.</p> <p>CVE ID : CVE-2021-25668</p>		
Out-of-bounds Write	22-04-2021	7.5	<p>A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl.</p>	<p>https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf</p>	O-SIE-SCAL-040521/927

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution.		

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-25669		
scalance_x208pro_firmware					
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE	https://certportal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/928

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code.</p> <p>CVE ID : CVE-2021-25668</p>		
Out-of-bounds Write	22-04-2021	7.5	<p>A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All</p>	<p>https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf</p>	O-SIE-SCAL-040521/929

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution.</p> <p>CVE ID : CVE-2021-25669</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
scalance_x212-2_firmware											
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/930						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code.</p> <p>CVE ID : CVE-2021-25668</p>		
Out-of-bounds Write	22-04-2021	7.5	<p>A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions),</p>	<p>https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf</p>	O-SIE-SCAL-040521/931

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					
			SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution. CVE ID : CVE-2021-25669							
scalance_x212-2ld_firmware										
Out-of-	22-04-2021	7.5	A vulnerability has been	https://cert-	O-SIE-SCAL-					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204	portal.siemens.com/productcert/pdf/ssa-187092.pdf	040521/932

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code. CVE ID : CVE-2021-25668		
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/933

CVSS Scoring Scale	0-1	1-2	2-3	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), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution. CVE ID : CVE-2021-25669		
scalance_x216_firmware					
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions <	https://cert-portal.siemens.com/prod	O-SIE-SCAL-040521/934

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions <	uctcert/pdf/ssa-187092.pdf	

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code. CVE ID : CVE-2021-25668		
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/935

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution.</p> <p>CVE ID : CVE-2021-25669</p>		
scalance_x224_firmware					
Out-of-bounds Write	22-04-2021	7.5	<p>A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1),</p>	https://certportal.siemens.com/productcert/pdf/ssa-	O-SIE-SCAL-040521/936

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant)	187092.pdf	

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code. CVE ID : CVE-2021-25668		
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-	https://certportal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/937

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution.</p> <p>CVE ID : CVE-2021-25669</p>		
scalance_xf201-3p_irt_firmware					
Out-of-bounds Write	22-04-2021	7.5	<p>A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1),</p>	<p>https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf</p>	O-SIE-SCAL-040521/938

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All		

CVSS Scoring Scale	0-1	1-2	2-3	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 < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code. CVE ID : CVE-2021-25668		
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions),	https://certportal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/939

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution.</p> <p>CVE ID : CVE-2021-25669</p>		
scalance_xf202-2p_irt_firmware					
Out-of-bounds Write	22-04-2021	7.5	<p>A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1),</p>	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/940

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All		

CVSS Scoring Scale	0-1	1-2	2-3	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), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code. CVE ID : CVE-2021-25668		
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/941

CVSS Scoring Scale	0-1	1-2	2-3	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), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution. CVE ID : CVE-2021-25669		

scalance_xf204_firmware

Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant)	https://certportal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/942
---------------------	------------	-----	---	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect		

CVSS Scoring Scale	0-1	1-2	2-3	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 of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code. CVE ID : CVE-2021-25668		
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions),	https://certportal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/943

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
			<p>SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution.</p> <p>CVE ID : CVE-2021-25669</p>		

scalance_xf204_irt_firmware

Out-of-bounds Write	22-04-2021	7.5	<p>A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT</p>	<p>https://certportal.siemens.com/productcert/pdf/ssa-187092.pdf</p>	O-SIE-SCAL-040521/944
---------------------	------------	-----	--	--	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204- 2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204- 2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206- 1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212- 2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202- 2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver		

CVSS Scoring Scale	0-1	1-2	2-3	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 result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code. CVE ID : CVE-2021-25668		
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All	https://certportal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/945

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution. CVE ID : CVE-2021-25669		
scalance_xf204-2_firmware					
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/946

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker		

CVSS Scoring Scale	0-1	1-2	2-3	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 leverage this to cause denial-of-service on the device and potentially remotely execute code. CVE ID : CVE-2021-25668		
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions),	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/947

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution.</p> <p>CVE ID : CVE-2021-25669</p>		

scalance_xf204-2ba_irt_firmware

Out-of-bounds Write	22-04-2021	7.5	<p>A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO</p>	<p>https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf</p>	O-SIE-SCAL-040521/948
---------------------	------------	-----	--	--	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device and potentially remotely execute code. CVE ID : CVE-2021-25668		
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/949

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution. CVE ID : CVE-2021-25669		

scalance_xf206-1_firmware

Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl.	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/950
---------------------	------------	-----	---	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code.		

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-25668								
Out-of-bounds Write	22-04-2021	7.5	A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-	https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf	O-SIE-SCAL-040521/951						
CVSS Scoring Scale		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution.</p> <p>CVE ID : CVE-2021-25669</p>		

scalance_xf208_firmware

Out-of-bounds Write	22-04-2021	7.5	<p>A vulnerability has been identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions),</p>	<p>https://cert-portal.siemens.com/productcert/pdf/ssa-187092.pdf</p>	O-SIE-SCAL-040521/952
---------------------	------------	-----	--	--	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204 (All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the webserver may result in write out of bounds in heap. An attacker might leverage this to cause denial-of-service on the device and potentially remotely execute code.</p> <p>CVE ID : CVE-2021-25668</p>		
Out-of-	22-04-2021	7.5	A vulnerability has been	https://cert-	O-SIE-SCAL-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			identified in SCALANCE X200-4P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT (All versions < 5.5.1), SCALANCE X201-3P IRT PRO (All versions < 5.5.1), SCALANCE X202-2 IRT (All versions < 5.5.1), SCALANCE X202-2P IRT (incl. SIPLUS NET variant) (All versions < 5.5.1), SCALANCE X202-2P IRT PRO (All versions < 5.5.1), SCALANCE X204 IRT (All versions < 5.5.1), SCALANCE X204 IRT PRO (All versions < 5.5.1), SCALANCE X204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2FM (All versions), SCALANCE X204-2LD (incl. SIPLUS NET variant) (All versions), SCALANCE X204-2LD TS (All versions), SCALANCE X204-2TS (All versions), SCALANCE X206-1 (All versions), SCALANCE X206-1LD (All versions), SCALANCE X208 (incl. SIPLUS NET variant) (All versions), SCALANCE X208PRO (All versions), SCALANCE X212-2 (incl. SIPLUS NET variant) (All versions), SCALANCE X212-2LD (All versions), SCALANCE X216 (All versions), SCALANCE X224 (All versions), SCALANCE XF201-3P IRT (All versions < 5.5.1), SCALANCE XF202-2P IRT (All versions < 5.5.1), SCALANCE XF204	portal.siemens.com/productcert/pdf/ssa-187092.pdf	040521/953

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(All versions), SCALANCE XF204 IRT (All versions < 5.5.1), SCALANCE XF204-2 (incl. SIPLUS NET variant) (All versions), SCALANCE XF204-2BA IRT (All versions < 5.5.1), SCALANCE XF206-1 (All versions), SCALANCE XF208 (All versions). Incorrect processing of POST requests in the web server may write out of bounds in stack. An attacker might leverage this to denial-of-service of the device or remote code execution. CVE ID : CVE-2021-25669		
simotics_connect_400_firmware					
Use of Insufficiently Random Values	22-04-2021	5	A vulnerability has been identified in Nucleus 4 (All versions < V4.1.0), Nucleus NET (All versions), Nucleus RTOS (versions including affected DNS modules), Nucleus ReadyStart (All versions < V2017.02.3), Nucleus Source Code (versions including affected DNS modules), SIMOTICS CONNECT 400 (All versions < V0.5.0.0), SIMOTICS CONNECT 400 (All versions >= V0.5.0.0), VSTAR (versions including affected DNS modules). The DNS client does not properly randomize DNS transaction IDs. That could allow an attacker to poison the DNS cache or spoof DNS resolving.	https://cert-portal.siemens.com/productcert/pdf/ssa-705111.pdf , https://cert-portal.siemens.com/productcert/pdf/ssa-669158.pdf	O-SIE-SIMO-040521/954

CVSS Scoring Scale	0-1	1-2	2-3	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-2021-25677		
tendacn					
g0_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-04-2021	10	<p>Command Injection in Tenda G0 routers with firmware versions v15.11.0.6(9039)_CN and v15.11.0.5(5876)_CN , and Tenda G1 and G3 routers with firmware versions v15.11.0.17(9502)_CN or v15.11.0.16(9024)_CN allows remote attackers to execute arbitrary OS commands via a crafted action/setDebugCfg request. This occurs because the "formSetDebugCfg" function executes glibc's system function with untrusted input.</p> <p>CVE ID : CVE-2021-27691</p>	N/A	O-TEN-G0_F-040521/955
g1_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-04-2021	10	<p>Command Injection in Tenda G0 routers with firmware versions v15.11.0.6(9039)_CN and v15.11.0.5(5876)_CN , and Tenda G1 and G3 routers with firmware versions v15.11.0.17(9502)_CN or v15.11.0.16(9024)_CN allows remote attackers to execute arbitrary OS commands via a crafted action/setDebugCfg request. This occurs because the "formSetDebugCfg" function executes glibc's system function with untrusted</p>	N/A	O-TEN-G1_F-040521/956

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			input. CVE ID : CVE-2021-27691							
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-04-2021	10	Command Injection in Tenda G1 and G3 routers with firmware versions v15.11.0.17(9502)_CN or v15.11.0.16(9024)_CN allows remote attackers to execute arbitrary OS commands via a crafted "action/umountUSBPartition" request. This occurs because the "formSetUSBPartitionUmount" function executes the "doSystemCmd" function with untrusted input. CVE ID : CVE-2021-27692	N/A	O-TEN-G1_F-040521/957					
g3_firmware										
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-04-2021	10	Command Injection in Tenda G0 routers with firmware versions v15.11.0.6(9039)_CN and v15.11.0.5(5876)_CN , and Tenda G1 and G3 routers with firmware versions v15.11.0.17(9502)_CN or v15.11.0.16(9024)_CN allows remote attackers to execute arbitrary OS commands via a crafted action/setDebugCfg request. This occurs because the "formSetDebugCfg" function executes glibc's system function with untrusted input. CVE ID : CVE-2021-27691	N/A	O-TEN-G3_F-040521/958					
Improper Neutralization of Special	16-04-2021	10	Command Injection in Tenda G1 and G3 routers with firmware versions	N/A	O-TEN-G3_F-040521/959					
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			v15.11.0.17(9502)_CN or v15.11.0.16(9024)_CN allows remote attackers to execute arbitrary OS commands via a crafted "action/umountUSBPartition" request. This occurs because the "formSetUSBPartitionUmount" function executes the "doSystemCmd" function with untrusted input. CVE ID : CVE-2021-27692		

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