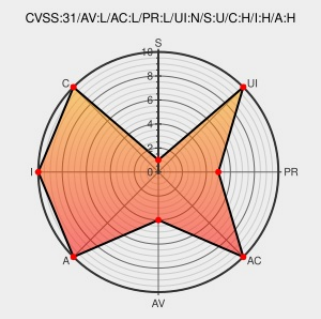
CVE-2022-22251

Published on: Not Yet Published

Last Modified on: 10/21/2022 05:08:00 PM UTC

CVE-2022-22251 - advisory for JSA69908

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Csrx from Juniper contain the following vulnerability:

On cSRX Series devices software permission issues in the container filesystem and stored files combined with storing passwords in a recoverable format in Juniper Networks Junos OS allows a local, low-privileged attacker to elevate their permissions to take control of any instance of a cSRX software deployment. This issue affects Juniper Networks Junos OS 20.2 version 20.2R1 and later versions prior to 21.2R1 on cSRX Series.

CVE-2022-22251 has been assigned by sirt@juniper.net to track the vulnerability - currently rated as HIGH severity.

Juniper SIRT is not aware of any malicious exploitation of this vulnerability.

Affected Vendor/Software: **Juniper Networks** - **Junos OS** version **>= 20.2R1**

Affected Vendor/Software: **Juniper Networks** - **Junos OS** version **>= 20.3R1**

Affected Vendor/Software: **Juniper Networks** - **Junos OS** version **>= 20.4R1**

Affected Vendor/Software: **Juniper Networks** - **Junos OS** version **>= 21.1R1**

Affected Vendor/Software: **Juniper Networks** - **Junos OS** version **!< 20.2R1**

Vulnerability Patch/Work Around

There are no viable workarounds for this issue. To reduce the risk of exploitation of this issue, use access lists or firewall filters to limit access to the cSRX instance to only trusted administrative networks, hosts and users.

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**

UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
CEC Juniper Community	kb.juniper.net text/html	CONFIRM kb.juniper.net/JSA69908

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Juniper	Csrx	-	All	All	All
Operating System	Juniper	Junos	All	All	All	All

cpe:2.3:h:juniper:csrx:-:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@sidfm_jp	Juniper Networks cSRX シリーズの Junos OS に権限を昇格される問題 (CVE-2022-22251) [43624] sid.softek.jp/content/show/4… #SIDfm #脆弱性情報	2022-10-17 08:30:06
@CVEreport	CVE-2022-22251 : On cSRX Series devices software permission issues in the container filesystem and stored files com… twitter.com/i/web/status/1…	2022-10-18 03:04:32
/r/netcve	CVE-2022-22251	2022-10-18 03:38:56

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report