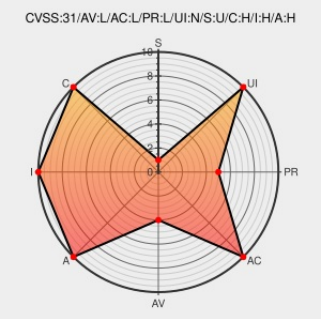
CVE-2021-31357

Published on: 10/19/2021 12:00:00 AM UTC

Last Modified on: 10/24/2022 06:45:00 PM UTC

CVE-2021-31357 - advisory for JSA11221

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



Certain versions of Junos Os Evolved from Juniper contain the following vulnerability:

A command injection vulnerability in tcpdump command processing on Juniper Networks Junos OS Evolved allows an attacker with authenticated CLI access to be able to bypass configured access protections to execute arbitrary shell commands within the context of the current user. The vulnerability allows an attacker to bypass command authorization restrictions assigned to their specific user account and execute commands that are available to the privilege level for which the user is assigned. For example, a user that is in the super-user login class, but restricted to executing specific CLI commands could exploit the vulnerability to execute any other command available to an unrestricted admin user. This vulnerability does not increase the privilege level of the user, but rather bypasses any CLI command restrictions by allowing full access to the shell. This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.3R2-S1-EVO; 20.4 versions prior to 20.4R2-S2-EVO; 21.1 versions prior to 21.1R2-EVO; 21.2 versions prior to 21.2R1-S1-EVO, 21.2R2-EVO.

CVE-2021-31357 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 Evolved** version **< 20.3R2-S1-EVO**

Affected Vendor/Software: **Juniper Networks** - **Junos OS Evolved** version **< 20.4R2-S2-EVO**

Affected Vendor/Software: **Juniper Networks** - **Junos OS Evolved** version **< 21.1R2-EVO**

Affected Vendor/Software: **Juniper Networks** - **Junos OS Evolved** version **< 21.2R1-S1-EVO, 21.2R2-EVO**

Vulnerability Patch/Work Around

Use access lists or firewall filters to limit access to the device via CLI only from trusted hosts and from trusted administrators. Limit access to the 'monitor traffic' command to authorized administrators.

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

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
2021-10 Security Bulletin: Junos OS Evolved: Multiple shell-injection vulnerabilities in EVO UI wrapper scripts - Juniper Networks	kb.juniper.net text/html	CONFIRM kb.juniper.net/JSA11221

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Juniper	Junos Os Evolved	20.4	r1	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r1-s1	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r1-s2	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r2	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r2-s1	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r2-s2	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r2-s3	All	All

Operating System	Juniper	Junos Os Evolved	20.4	r3	All	All
Operating System	Juniper	Junos Os Evolved	21.1	-	All	All
Operating System	Juniper	Junos Os Evolved	21.1	r1	All	All
Operating System	Juniper	Junos Os Evolved	21.1	r1-s1	All	All
Operating System	Juniper	Junos Os Evolved	21.1	r2	All	All
Operating System	Juniper	Junos Os Evolved	21.2	r1	All	All
Operating System	Juniper	Junos Os Evolved	21.2	r1-s1	All	All
Operating System	Juniper	Junos Os Evolved	21.2	r2	All	All
Operating System	Juniper	Junos Os Evolved	All	All	All	All

cpe:2.3:o:juniper:junos_os_evolved:20.4:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:20.4:r1-s1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:20.4:r1-s2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:20.4:r2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:20.4:r2-s1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:20.4:r2-s2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:20.4:r2-s3:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:20.4:r3:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:21.1:-:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:21.1:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:21.1:r1-s1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:21.1:r2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:21.2:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:21.2:r1-s1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:21.2:r2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-31357 : A command injection vulnerability in tcpdump command processing on Juniper Networks Junos OS Evolv… twitter.com/i/web/status/1…	2021-10-19 18:29:42

← Previous ID

Next ID→