مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Exploited Vulnerability in Juniper Networks Junos OS

Tracking #:432316971

Date:14-03-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a security vulnerability in Juniper Networks Junos OS. This vulnerability allows a local attacker with shell access and high privileges to execute arbitrary code, potentially compromising the integrity of the device.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2025-21590**
- CVSS Score 6.7 Medium
- A critical privilege escalation vulnerability in Juniper Networks Junos OS, enabling local attackers with shell access to execute arbitrary code and compromise device integrity. This vulnerability has been actively exploited in the wild.
- The flaw stems from **improper isolation in Junos OS kernel**, allowing authenticated local attackers with high privileges to bypass security restrictions through shell access.
- Exploitation requires **local shell access**; not exploitable via the Junos CLI.

Affected Versions:

Affects all listed Junos OS versions;

- All versions before 21.2R3-S9,
- 21.4 versions before 21.4R3-S10,
- 22.2 versions before 22.2R3-S6,
- 22.4 versions before 22.4R3-S6,
- 23.2 versions before 23.2R2-S3,
- 23.4 versions before 23.4R2-S4,
- 24.2 versions before 24.2R1-S2, 24.2R2.

Junos OS Evolved is unaffected.

Mitigations:

Upgrade to one of the following fixed releases:

- **21.2R3-S9*** (future release)
- **21.4R3-S10**
- **22.2R3-S6**
- **22.4R3-S6**
- **23.2R2-S3**
- **23.4R2-S4*** (future release)
- **24.2R1-S2**
- **24.2R2**
- **24.4R1** and all subsequent releases

Notes:

Juniper Networks Stated that:

- The complete list of resolved platforms is under investigation.
- **EOE/EOL releases will not be evaluated or patched**.

Workaround: Restrict **shell access to trusted users only** until upgrades are applied.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by Juniper Networks.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://supportportal.juniper.net/s/article/2025-03-Out-of-Cycle-Security-Bulletin-Junos-OS-A-local-attacker-with-shell-access-can-execute-arbitrary-code-CVE-2025-21590?language=en_US