Support Portal

2026-04 Security Bulletin: Junos OS: MX Series: Missing Authorization for specific 'request' CLI commands in a JDM/CSDS scenario (CVE-2026-33785)

Article ID JSA107872 **Created** 2026-04-08 **Last Updated** 2026-04-09

Product Affected

This issue affects Junos OS 24.4, 25.2. Affected platforms: MX Series.

Severity
High

Severity Assessment (CVSS) Score
CVSS: v3.1: 8.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) **CVSS: v4.0:** 6.3 (CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:H/SI:H/SA:H/AU:Y/R:U/RE:M)

Problem

A Missing Authorization vulnerability in the CLI of Juniper Networks Junos OS on MX Series allows a local, authenticated user with low privileges to execute specific commands which will lead to a complete compromise of managed devices.

Any user logged in, without requiring specific privileges, can issue 'request csds' CLI operational commands. These commands are only meant to be executed by high privileged or users designated for Juniper Device Manager (JDM) / Connected Security Distributed Services (CSDS) operations as they will impact all aspects of the devices managed via the respective MX.

This issue affects Junos OS on MX Series:

- 24.4 releases before 24.4R2-S3,
- 25.2 releases before 25.2R2.

This issue does not affect Junos OS releases before 24.4.

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

This issue was found during internal product security testing or research.

Solution

The following software releases have been updated to resolve this specific issue: 24.4R2-S3, 25.2R2, 25.4R1, and all subsequent releases.

This issue is being tracked as 1914935 which is visible on the Customer Support website.

Note: Juniper SIRT's policy is not to evaluate releases which are beyond End of Engineering (EOE) or End of Life (EOL).

Workaround

Use access lists or firewall filters to limit access to the CLI only from trusted hosts and administrators.

Utilize CLI authorization to disallow execution of the 'request csds' commands.

Severity Assessment

Information for how Juniper Networks uses CVSS can be found at KB 16446 "Common Vulnerability Scoring System (CVSS) and Juniper's Security Advisories."

Modification History

```
2026-04-08: Initial Publication
```

Related Information

- KB16613: Overview of the Juniper Networks SIRT Quarterly Security Bulletin Publication Process
- KB16765: In which releases are vulnerabilities fixed?
- KB16446: Common Vulnerability Scoring System (CVSS) and Juniper's Security Advisories
- Report a Security Vulnerability - How to Contact the Juniper Networks Security Incident Response Team

AFFECTED PRODUCT SERIES / FEATURES