Junos OS: MX Series: Missing Authorization for specific 'request' CLI commands in a JDM/CSDS scenario

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-33785
State	PUBLISHED
Assigner	juniper
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-09 22:16:27 UTC
Updated	2026-04-09 22:16:27 UTC
Description	A Missing Authorization vulnerability in the CLI of Juniper Networks Junos OS on MX Series allows a local, authenticated us

Risk And Classification

Primary CVSS: v4.0 6.3 MEDIUM from sirt@juniper.net

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/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:Y/R:U/V:X/RE:M/U:X

EPSS: 0.000120000 probability, percentile 0.016620000 (date 2026-04-10)

Problem Types: CWE-862 | CWE-862 CWE-862 Missing Authorization

Version	Source	Type	Score	Severity	Vector
4.0	sirt@juniper.net	Secondary	6.3	MEDIUM	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/E:X/C...
4.0	CNA	CVSS	6.3	MEDIUM	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/...
3.1	sirt@juniper.net	Primary	8.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	CVSS	8.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Privileges Required

Low

User Interaction

None

Confidentiality

None

Integrity

Low

Availability

None

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

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/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:Y/R:U/V:X/RE:M/U:X

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Juniper Networks	Junos OS	affected 24.4 24.4R2-S3 semver	MX Series
CNA	Juniper Networks	Junos OS	affected 25.2 25.2R2 semver	MX Series

CNA	Juniper Networks	Junos OS	unaffected 24.4R1 semver	MX Series

References

Reference	Source	Link	Tags
kb.juniper.net/JSA107872	sirt@juniper.net	kb.juniper.net	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Solutions

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

Workarounds

CNA: 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.

Exploits

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

There are currently no legacy QID mappings associated with this CVE.