JUNIPER NETWORKS | Support Portal

Product Affected

This issue affects all versions of Junos OS. Affected platforms: MX Series.

Severity
Medium

Severity Assessment (CVSS) Score
CVSS: v3.1: 6.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)
CVSS: v4.0: 6.9 (CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N/AU:Y/R:U/RE:L)

Problem

An Improper Check for Unusual or Exceptional Conditions vulnerability in the packet forwarding engine (pfe) of Juniper Networks Junos OS on MX Series allows an unauthenticated, network-based attacker to bypass the configured firewall filter and access the control-plane of the device.

On MX platforms with MPC10, MPC11, LC4800 or LC9600 line cards, and MX304, firewall filters applied on a loopback interface lo0.n (where n is a non-0 number) don't get executed when lo0.n is in the global VRF / default routing-instance.

An affected configuration would be:

```
user@host# show configuration interfaces lo0 | display set
set interfaces lo0 unit 1 family inet filter input <filter-name>
```

where a firewall filter is applied to a non-0 loopback interface, but that loopback interface is not referred to in any routing-instance (RI) configuration, which implies that it's used in the default RI.

The issue can be observed with the CLI command:

```
user@device> show firewall counter filter <filter_name>
```

not showing any matches.

This issue affects Junos OS on MX Series:

- all versions before 23.2R2-S6,
- 23.4 versions before 23.4R2-S7,
- 24.2 versions before 24.2R2,
- 24.4 versions before 24.4R2.

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

This issue was seen during production usage.

Solution

The following software releases have been updated to resolve this specific issue: 23.2R2-S6, 23.4R2-S7, 24.2R2, 24.4R2, 25.2R1, and all subsequent releases.

This issue is being tracked as 1855648 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

Renaming the lo0 logical unit used in the default routing instance from non-0 to 0 resolves this issue.

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