مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# High-Severity Vulnerability in Juniper Networks Junos OS

Tracking #:432318310

Date:26-01-2026

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability affecting Juniper Networks Junos OS and Junos OS Evolved that could allow a DHCP client to exhaust IP address pools across multiple subnets, potentially resulting in a denial-of-service (DoS) condition on downstream DHCP servers.

## TECHNICAL DETAILS:

**Vulnerability Details**

- **CVE-2025-59960**
- **CVSS v3.1 Score:** 7.4 (High)
- An Improper Check for Unusual or Exceptional Conditions vulnerability exists in the Juniper DHCP service (jdhcpd). When DHCP relay is configured in forward-only mode, the device incorrectly forwards DHCP DISCOVER messages containing client-supplied Option 82 information without modification, even when the trust-option82 setting is not enabled.
- As a result, a DHCP client in one subnet can consume IP address leases intended for other subnets, leading to address pool exhaustion and service disruption on the DHCP server.

**Affected Products**

**Junos OS**

- All versions before **21.2R3-S10**
- 21.4 before **21.4R3-S12**
- All versions of **22.2**
- 22.4 before **22.4R3-S8**
- 23.2 before **23.2R2-S5**
- 23.4 before **23.4R2-S6**
- 24.2 before **24.2R2-S2**
- 24.4 before **24.4R2**
- 25.2 before **25.2R1-S1**, **25.2R2**

**Junos OS Evolved**

- All versions before **21.4R3-S12-EVO**
- All versions of **22.2-EVO**
- 22.4 before **22.4R3-S8-EVO**
- 23.2 before **23.2R2-S5-EVO**
- 23.4 before **23.4R2-S6-EVO**
- 24.2 before **24.2R2-S2-EVO**
- 24.4 before **24.4R2-EVO**
- 25.2 before **25.2R1-S1-EVO**, **25.2R2-EVO**

**Fixed Versions**

- Junos OS 21.2R3-S10, 21.4R3-S12, 22.4R3-S8, 23.2R2-S5, 23.4R2-S6, 24.2R2-S2, 24.4R2, 25.2R1-S1, 25.2R2, 25.4R1, and later.
- Junos OS Evolved 21.4R3-S12-EVO, 22.4R3-S8-EVO, 23.2R2-S5-EVO, 23.4R2-S6-EVO, 24.2R2-S2-EVO, 24.4R2-EVO, 25.2R1-S1-EVO, 25.2R2-EVO, 25.4R1-EVO, and later.

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released 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/2026-01-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-DHCP-Option-82-messages-from-clients-being-passed-unmodified-to-the-DHCP-server-CVE-2025-59960