مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Security Updates – Juniper Junos OS

Tracking #:432316737

Date:14-01-2025



TLP: WHITE

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Juniper Networks has recently disclosed two high-severity vulnerabilities in their Junos OS and Junos OS Evolved systems.

## TECHNICAL DETAILS:

Juniper Networks has recently disclosed two high-severity vulnerabilities in their Junos OS and Junos OS Evolved systems: CVE-2025-21598 and CVE-2025-21599. These vulnerabilities are critical because they can be exploited by unauthenticated attackers, posing a significant risk of Denial of Service (DoS) attacks and network-wide disruptions.Both vulnerabilities have been assigned a CVSSv3 score of 7.5, indicating high severity.

**Vulnerability Details:**

1. CVE-2025-21598: Out-of-Bounds Read in Routing Protocol Daemon (RPD)
   - Affected Systems: Junos OS versions 21.2R3-S8 through 24.2R1 and corresponding versions of Junos OS Evolved.
   - Description: This vulnerability occurs in the routing protocol daemon (RPD) and allows unauthenticated attackers to send malformed Border Gateway Protocol (BGP) packets, causing RPD to crash. The attack can spread across multiple Autonomous Systems (ASes), potentially impacting interconnected networks. Devices with BGP trace options enabled are especially vulnerable.

2. CVE-2025-21599: Memory Exhaustion in Juniper Tunnel Driver (jtd)
   - Affected Systems: from 22.4-EVO before 22.4R3-S5-EVO,
     - from 23.2-EVO before 23.2R2-S2-EVO,
     - from 23.4-EVO before 23.4R2-S2-EVO,
     - from 24.2-EVO before 24.2R1-S2-EVO, 24.2R2-EVO.
   - Fixed Version:
     - Junos OS Evolved: 22.4R3-S5-EVO, 23.2R2-S2-EVO, 23.4R2-S2-EVO, 24.2R1-S2-EVO, 24.2R2-EVO, 24.4R1-EVO, and all subsequent releases.
   - Description: A memory exhaustion vulnerability exists in the Juniper Tunnel Driver (jtd) where specially crafted IPv6 packets can cause kernel memory exhaustion. This leads to a Denial of Service (DoS) condition as continuous receipt of malicious packets depletes available system memory, causing the system to crash.

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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/JSA92869
- https://supportportal.juniper.net/JSA92867