مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Bulletin: Junos OS and Junos OS Evolved

Tracking #:432317480

Date:14-07-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Juniper Networks has disclosed a medium-severity vulnerability (CVE-2025-52953) in Junos OS and Junos OS Evolved that affects BGP (Border Gateway Protocol) session handling.

TECHNICAL DETAILS:

Juniper Networks has disclosed a medium-severity vulnerability (CVE-2025-52953) in Junos OS and Junos OS Evolved that affects BGP (Border Gateway Protocol) session handling. An unauthenticated, adjacent attacker can exploit the flaw by sending a crafted yet valid BGP UPDATE packet, forcing the BGP session to reset. Repeated exploitation may result in a sustained Denial of Service (DoS) condition, potentially affecting critical network routing functionality. Both iBGP and eBGP configurations, and IPv4 and IPv6, are impacted.

Vulnerability Details:

- CVE ID: CVE-2025-52953
- CVSS Score:v4.0: 7.1 (AV:A/AC:L/AT:N/PR:N/UI:N/VA:H/SA:L/R:A/V:C/RE:M/U:Amber)
- Impact: Denial of Service through BGP session reset
- Attack Vector: Adjacent network (e.g., directly connected peers)
- Exploitation Status: Not observed in the wild
- Affected Components: Routing Protocol Daemon (rpd)
- Protocols Affected: iBGP, eBGP, IPv4, IPv6
- Exposure Criteria: Systems configured with inet6-vpn unicast BGP families

Patched Versions:

Junos OS: Junos OS: 21.2R3-S9, 21.4R3-S11, 22.2R3-S7, 22.4R3-S7, 23.2R2-S4, 23.4R2-S4, 24.2R2, 24.4R1-S3, 24.4R2, 25.2R1, and all subsequent releases.

Junos OS Evolved: 22.2R3-S7-EVO, 22.4R3-S7-EVO, 23.2R2-S4-EVO, 23.4R2-S4-EVO, 24.2R2-EVO, 24.4R1-S3-EVO, 24.4R2-EVO, 25.2R1-EVO, and all subsequent releases.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade Junos OS and Junos OS Evolved to the patched 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/s/article/2025-07-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-An-unauthenticated-adjacent-attacker-sending-a-valid-BGP-UPDATE-packet-forces-a-BGP-session-reset-CVE-2025-52953?language=en_US