مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - Juniper Networks

Tracking #:432317059

Date:10-04-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Juniper Networks has released security updates to address multiple vulnerabilities in its products.

TECHNICAL DETAILS:

Multiple vulnerabilities have been identified in Junos OS and Junos OS Evolved platforms. These vulnerabilities can lead to Denial of Service (DoS), memory leaks, process crashes, unauthorized access to sensitive information, and other security impacts. Exploitation of these vulnerabilities could severely impact network operations and compromise the integrity of affected devices.

High Severity Vulnerabilities:

- JSA96455 (CVE-2025-30645): Junos OS: SRX Series: Transmission of specific control traffic sent out of a DS-Lite tunnel results in flowd crash. Exploitation could lead to a denial of service on SRX Series devices.
- JSA96469 (CVE-2025-30658): Junos OS: SRX Series: On devices with Anti-Virus enabled, malicious server responses will cause memory to leak ultimately causing forwarding to stop. This issue can lead to a denial of service on SRX Series devices with Anti-Virus enabled.
- JSA96470 (CVE-2025-30659): Junos OS: SRX Series: A device configured for vector routing crashes when receiving specific traffic. Exploitation can result in a denial of service on SRX Series devices configured for vector routing.
- JSA96471 (CVE-2025-30660): Junos OS: MX Series: Decapsulation of specific GRE packets leads to PFE reset. This vulnerability can cause a denial of service on MX Series devices.
- JSA96449 (CVE-2025-21594): Junos OS: MX Series: In DS-lite and NAT scenario receipt of crafted IPv4 traffic causes port block. Exploitation can lead to a denial of service on MX Series devices in specific DS-lite and NAT configurations.
- JSA96466 (CVE-2025-30656): Junos OS: MX Series, SRX Series: Processing of specific SIP INVITE messages by the SIP ALG will lead to an FPC crash. This can result in a denial of service on affected MX and SRX Series devices.
- JSA96459 (CVE-2025-30649): Junos OS: MX240, MX480, MX960 with SPC3: An attacker sending specific packets will cause a CPU utilization DoS. This vulnerability can lead to a denial of service on specific MX Series devices with SPC3.

Note: Refer to the Juniper Networks advisory for additional CVEs, fixed versions, and further information.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided 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/global-search/%40uri?language=en_US#sort=%40sfcec_community_publish_date_formula__c%20descending&f:ctype=[Security%20Advisories]