مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Juniper Products

Tracking #:432316005

Date:02-07-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Juniper released a security update to address a critical vulnerability in its products.

TECHNICAL DETAILS:

Juniper Networks has released an emergency update to address a critical severity vulnerability that leads to authentication bypass in Session Smart Router (SSR), Session Smart Conductor, and WAN Assurance Router products.

Vulnerability Details:

- **CVE-2024-2973**| CVSS score: 10 - Critical
- An Authentication Bypass Using an Alternate Path or Channel vulnerability in Juniper Networks Session Smart Router or Conductor running with a redundant peer allows a network-based attacker to bypass authentication and take full control of the device.
- Only Routers or Conductors that are running in high-availability redundant configurations are affected by this vulnerability.

Affected versions:

- **Session Smart Router & Conductor:**
  - All versions before 5.6.15
  - From 6.0 before 6.1.9-lts
  - From 6.2 before 6.2.5-sts

- **WAN Assurance Router:**
  - 6.0 versions before 6.1.9-lts
  - 6.2 versions before 6.2.5-sts

Fixed versions:

- **Session Smart Router & Conductor:**
  - SSR-5.6.15
  - SSR-6.1.9-lts
  - SSR-6.2.5-sts, and subsequent releases.

- **WAN Assurance Router:**
  - Patched automatically when connected to the Mist Cloud.
  - High-Availability clusters need to upgrade to SSR-6.1.9 or SSR-6.2.5

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Juniper.

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/2024-06-Out-Of-Cycle-Security-Bulletin-Session-Smart-Router-SSR-On-redundant-router-deployments-API-authentication-can-be-bypassed-CVE-2024-2973?language=en_US