CERT-EU

Security Advisory 2024-065

Critical Vulnerability in Juniper Networks Products

July 1, 2024 — v1.0

TLP:CLEAR

History:

- *01/07/2024 — v1.0 – Initial publication*

Summary

On June 27, 2024, Juniper Networks issued an advisory about a critical vulnerability, **CVE-2024-2973**, affecting Session Smart Router (SSR), Session Smart Conductor, and WAN Assurance Router products. This vulnerability allows an attacker to bypass authentication and gain full control of the device, primarily affecting high-availability redundant configurations [1].

It is recommended to update affected devices immediately.

Technical Details

The vulnerability, **CVE-2024-2973**, is an authentication bypass using an alternate path or channel. It affects Juniper Networks SSR and Conductor running in high-availability configurations, allowing attackers to bypass authentication and take control of the device [1].

Affected Products

- Session Smart Router & Conductor:
- – All versions before 5.6.15
  – 6.0 before 6.1.9-lts
  – 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

Recommendations

CERT-EU recommends updating affected devices to the latest versions as soon as possible.

References

[1] https://www.bleepingcomputer.com/news/security/juniper-releases-out-of-cycle-fix-for-max-severity-auth-bypass-flaw/