National Cyber Security Centre

2407010177-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical Vulnerability exists in Juniper Networks Session Smart Router, Session Smart Conductor and WAN Assurance Router

Monday 1st July, 2024

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.*
For more information on the Traffic Light Protocol, see https://www.first.org/tlp/.
Please treat this document in accordance with the TLP assigned.

Description

Published: 2024-06-27T21:15:00
Vendor: Juniper Networks
Product: Session Smart Router Session Smart Conductor WAN Assurance Router
CVE ID: CVE-2024-2973
CVSS 3.0 Score[1]**:** 10
EPSS[2]**:** 0.392770000

Summary: 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.

More information related to this issue can be found at the following link(s):

- https://supportportal.juniper.net/JSA83126
- https://support.juniper.net/support/eol/software/ssr/

Products Affected

Session Smart Router:

- All versions before 5.6.15
- from 6.0 before 6.1.9-lts
- from 6.2 before 6.2.5-sts

Session Smart 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

No other Juniper Networks products or platforms are affected by this issue.

Impact

Common Weakness Enumeration (CWE)[3]**:**

- CWE-288 Authentication Bypass Using an Alternate Path or Channel

Present in CISA Known Exploited Vulnerability(KEV)[4] **catalog:** NO

[1] https://www.first.org/cvss/v3.0/specification-document
[2] https://www.first.org/epss/articles/prob_percentile_bins
[3] https://cwe.mitre.org/
[4] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Recommendations

The NCSC strongly advises affected organisations to review the latest release notes and install the relevant updates from Juniper Networks.

Additional recommendations and mitigation's for CVE-2024-2973 can be found in the respective links below:

- https://supportportal.juniper.net/JSA83126
- https://support.juniper.net/support/eol/software/ssr/

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
Tom Johnson House,
Beggars Bush,
Dublin, D04 A068,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre