National Cyber Security Centre

2401120209-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical Vulnerability in Juniper Networks Junos OS (CVSSv3: 9.8)

Friday 12th January, 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: 10th January 2024
Vendor: Juniper Networks
Product: Junos OS
CVE ID: CVE-2024-21591
CVSS v3.0[1] **Score:** 9.8
Summary: An Out-of-bounds Write vulnerability in J-Web of Juniper Networks Junos OS SRX Series and EX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS), or Remote Code Execution (RCE) and obtain root privileges on the device.

This issue is caused by use of an insecure function allowing an attacker to overwrite arbitrary memory.

More information related to this issue can be found at the following link:
https://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Security-Vulnerability-in-J-web-allows-a-preAuth-Remote-Code-Execution-CVE-2024-21591?language=en_US

Products Affected

This issue affects Juniper Networks Junos OS SRX Series and EX Series:

- Junos OS versions earlier than 20.4R3-S9;
- Junos OS 21.2 versions earlier than 21.2R3-S7;
- Junos OS 21.3 versions earlier than 21.3R3-S5;
- Junos OS 21.4 versions earlier than 21.4R3-S5;
- Junos OS 22.1 versions earlier than 22.1R3-S4;
- Junos OS 22.2 versions earlier than 22.2R3-S3;
- Junos OS 22.3 versions earlier than 22.3R3-S2;
- Junos OS 22.4 versions earlier than 22.4R2-S2, 22.4R3.

Impact

Denial of Service (DoS), Remote Code Execution (RCE)

Common Weakness Enumeration (CWE)[2]**:** CWE-787 Out-of-bounds Write
Present in CISA Known Exploited Vulnerability(KEV)[3] **catalog:** NO

Recommendations

The NCSC strongly advises affected organisations to review the latest release notes and install the relevant updates from Juniper Networks. The following software releases have been updated to resolve this

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

specific issue:

Junos OS: 20.4R3-S9, 21.2R3-S7, 21.3R3-S5, 21.4R3-S5, 22.1R3-S4, 22.2R3-S3, 22.3R3-S2, 22.4R2-S2, 22.4R3, 23.2R1-S1, 23.2R2, 23.4R1, and all subsequent releases.

Workaround: Disable J-Web, or limit access to only trusted hosts.

Additional recommendations and mitigation's for the CVE can be found in the respective link below:

https://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Security-Vulnerability-in-J-web-allows-a-preAuth-Remote-Code-Execution-CVE-2024-21591?language=en_US

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
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie