National Cyber Security Centre

2309050125-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Multiple vulnerabilities identified in Juniper Network devices

Tuesday 5th September, 2023

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

Juniper Networks has released a software update that address vulnerabilities CVE-2023-36844, CVE-2023-36845, CVE-2023-36846, and CVE-2023-36847. The vulnerabilities affect Junos OS on EX and SRX series devices respectively. By chaining exploitation of these vulnerabilities, an unauthenticated, network-based attacker may be able to remotely execute code on the devices.

Juniper have reported a proof of concept has been published and exploit attempts have been detected.

The Juniper Networks out-of-cycle security bulletin can be viewed here: https://supportportal.juniper.net/s/article/2023-08-Out-of-Cycle-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Multiple-vulnerabilities-in-J-Web-can-be-combined-to-allow-a-preAuth-Remote-Code-Execution?language=en_US

Products Affected

Juniper Networks has reported that the vulnerabilities affect the following devices:

SRX Series:

- All versions prior to 20.4R3-S8
- 21.1 version 21.1R1 and later versions
- 21.2 versions prior to 21.2R3-S6
- 21.3 versions prior to 21.3R3-S5
- 21.4 versions prior to 21.4R3-S5
- 22.1 versions prior to 22.1R3-S3
- 22.2 versions prior to 22.2R3-S2
- 22.3 versions prior to 22.3R2-S2, 22.3R3
- 22.4 versions prior to 22.4R2-S1, 22.4R3

EX Series:

- All versions prior to 20.4R3-S8
- 21.1 version 21.1R1 and later versions
- 21.2 versions prior to 21.2R3-S6
- 21.3 versions prior to 21.3R3-S5

- 21.4 versions prior to 21.4R3-S4
- 22.1 versions prior to 22.1R3-S3
- 22.2 versions prior to 22.2R3-S1
- 22.3 versions prior to 22.3R2-S2, 22.3R3
- 22.4 versions prior to 22.4R2-S1, 22.4R3

Impact

By chaining exploitation of these vulnerabilities, threat actors could achieve remote code execution on the devices.

Juniper Networks has reported that exploitation attempts have occurred, although have not been successful at the time of reporting.

Recommendations

The NCSC strongly advises affected organisations to implement the available patches and limit access to the web management interface to only trusted devices. Further information on a work around and mitigation steps that organisations can take can be found here:

- https://supportportal.juniper.net/s/article/2023-08-Out-of-Cycle-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Multiple-vulnerabilities-in-J-Web-can-be-combined-to-allow-a-preAuth-Remote-Code-Execution?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@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie