10 years CERT-EU

Security Advisory 2023-059

Multiple Junos OS Vulnerabilities

September 19, 2023 — v1.1

TLP:CLEAR

History:

- *29/08/2023 — v1.0 – Initial publication*
- *19/09/2023 — v1.1 – Summary and technical details update*

Summary

Juniper Networks has released fixes to address several vulnerabilities. These vulnerabilities could potentially be chained together to allow unauthorised remote code execution (RCE) on SRX and EX series devices. The combined CVSS score for these flaws is 9.8 (Critical) and a PoC exploit has been publicly released. Therefore, CERT-EU strongly advises users to promptly update their devices to the latest versions, or apply the provided workaround [1,2].

[Update] On September 18, a VulnCheck vulnerability researcher released another PoC exploit that only utilises one of the vulnerabilities, bypassing the need to upload files while still achieving remote code execution [4].

Technical Details

Juniper released a total of four medium-severity vulnerabilities in its EX switches and SRX firewalls. The security flaws were found in the J-Web interface that administrators can use to manage and configure Juniper devices on their networks.

By utilising a crafted request that does not require authentication, an attacker is able to upload arbitrary files via J-Web, leading to partial loss of integrity, which may allow chaining to other vulnerabilities.

A public exploit has been released exploiting the vulnerability in the following steps [2,3]:

1. A pre-authentication upload vulnerability can be used to upload an arbitrary PHP file to a restricted directory with a randomised file name.
2. Using the same vulnerable function, an attacker can upload a PHP configuration file (`.ini`) which points to and loads the PHP file from step 1 using the `auto_prepend_file` directive.
3. As all environment variables can be set via HTTP requests, an adversary may overwrite the environment variable `PHPRC` to load the PHP configuration file from step 2 and trigger the execution of the PHP function declared in step 1.

[Update] The second PoC, released on September 18, only utilises **CVE-2023-36845**, bypassing the need to upload files while still achieving remote code execution. It consists in only one curl command that will:

1. Set the PHPRC environment variable to `/dev/fd/0` (used by FreeBSD process to access their stdin).
2. Include the desired `php.ini` in the HTTP request (using the `auto_prepend_file` directive) to display sensitive data.
3. By also enabling the `allow_url_include` directive, one can use any protocol wrapper with `auto_prepend_file`, such as `data://` to provide the "second file" inline without the need to upload it.

Considering the second PoC, the severity score of **CVE-2023-36845** might be reconsidered as high, or critical.

Affected Products

These issues affect Juniper Networks Junos OS on 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;

These issues affect Juniper Networks Junos OS on 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.

Recommendations

For SRX series, the following releases have resolved the issues:

- 20.4R3-S8
- 21.2R3-S6
- 21.3R3-S5
- 21.4R3-S5
- 22.1R3-S3
- 22.2R3-S2
- 22.3R2-S2
- 22.3R3
- 22.4R2-S1
- 22.4R3
- 23.2R1
- All subsequent releases

For EX series, the following releases have resolved the issues:

- 20.4R3-S8
- 21.2R3-S6
- 21.3R3-S5
- 21.4R3-S4
- 22.1R3-S3
- 22.2R3-S1
- 22.3R2-S2
- 22.3R3
- 22.4R2-S1
- 22.4R3
- 23.2R1
- All subsequent releases

CERT-EU strongly recommends upgrading affected devices.

Workaround

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

References

[1] 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&ref=labs.watchtowr.com

[2] https://github.com/watchtowrlabs/juniper-rce_cve-2023-36844?ref=labs.watchtowr.com

[3] https://labs.watchtowr.com/cve-2023-36844-and-friends-rce-in-juniper-firewalls/

[4] https://vulncheck.com/blog/juniper-cve-2023-36845