Security Advisory 2024-008

Critical Vulnerabilities in Junos OS

January 15, 2024 — v1.0

TLP:CLEAR

History:

- *15/01/2024 — v1.0 – Initial publication*

Summary

On January 10, 2024, Juniper released a security advisory addressing a critical vulnerability that, if exploited, could lead to a Denial of Service (DoS), or Remote Code Execution (RCE) [1].

While Juniper SIRT is not aware of any malicious exploitation of this vulnerability, it is recommended upgrading as soon as possible.

Technical Details

The vulnerability `CVE-2024-21591`, with a CVSS score of 9.8, is due to an insecure function allowing an attacker to overwrite arbitrary memory. It allows a network-based attacker to cause a Denial of Service (DoS), or Remote Code Execution (RCE) and obtain root privileges on the device.

To be vulnerable, at least one of the following configurations needs to be used on the device:

- `[system services web-management http]`
- `[system services web-management https]`

Affected Products

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.

Recommendations

It is strongly recommended upgrading all Junos OS to one of the fixed versions (or newer). It is also recommended limiting the J-Web configuration interface access to only trusted hosts and networks.

Workaround

If the update is not possible, a workaround is possible by disabling J-Web, or limit J-Web access to only trusted hosts.

References

[1] 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