10 years CERT-EU

Security Advisory 2022-071

Junos OS: Multiple Vulnerabilities in J-Web

October 17, 2022 — v1.0

TLP:CLEAR

History:

- *17/10/2022 — v1.0 – Initial publication*

Summary

Multiple vulnerabilities have been found in the **J-Web component** of **Juniper Networks Junos OS**. One or more of these issues could lead to unauthorized local file access, cross-site scripting attacks, path injection and traversal, or local file inclusion [1, 2].

Technical Details

- **CVE-2022-22241** - **CVSS 8.1** - An Improper Input Validation vulnerability in the J-Web component of Juniper Networks Junos OS may allow an unauthenticated attacker to access data without proper authorization. Utilizing a crafted POST request, deserialization may occur which could lead to unauthorized local file access or the ability to execute arbitrary commands.
- **CVE-2022-22242** - CVSS 6.1 - A Cross-site Scripting (XSS) vulnerability in the J-Web component of Juniper Networks Junos OS allows an unauthenticated attacker to run malicious scripts reflected off of J-Web to the victim's browser in the context of their session within J-Web.
- **CVE-2022-22243** - CVSS 4.3 - An XPath Injection vulnerability due to Improper Input Validation in the J-Web component of Juniper Networks Junos OS allows an authenticated attacker to add an XPath command to the XPath stream, which may allow chaining to other unspecified vulnerabilities, leading to a partial loss of confidentiality.
- **CVE-2022-22244** - CVSS 5.3 - An XPath Injection vulnerability in the J-Web component of Juniper Networks Junos OS allows an unauthenticated attacker sending a crafted POST to reach the XPath channel, which may allow chaining to other unspecified vulnerabilities, leading to a partial loss of confidentiality.
- **CVE-2022-22245** - CVSS 4.3 - A Path Traversal vulnerability in the J-Web component of Juniper Networks Junos OS allows an authenticated attacker to upload arbitrary files to the device by bypassing validation checks built into Junos OS. The attacker should not be able to execute the file due to validation checks built into Junos OS. Successful exploitation of this vulnerability could lead to loss of file system integrity.

- **CVE-2022-22246** - CVSS 7.5 - A PHP Local File Inclusion (LFI) vulnerability in the J-Web component of Juniper Networks Junos OS may allow a low-privileged authenticated attacker to execute an untrusted PHP file. By chaining this vulnerability with other unspecified vulnerabilities, and by circumventing existing attack requirements, successful exploitation could lead to a complete system compromise.

Affected Products

These vulnerabilities affect the following Juniper Networks Junos OS:

- All versions prior to 19.1R3-S9;
- 19.2 versions prior to 19.2R3-S6;
- 19.3 versions prior to 19.3R3-S7;
- 19.4 versions prior to 19.4R3-S9;
- 20.1 versions prior to 20.1R3-S5;
- 20.2 versions prior to 20.2R3-S5;
- 20.3 versions prior to 20.3R3-S5;
- 20.4 versions prior to 20.4R3-S4;
- 21.1 versions prior to 21.1R3-S2;
- 21.2 versions prior to 21.2R3-S1;
- 21.3 versions prior to 21.3R3;
- 21.4 versions prior to 21.4R3;
- 22.1 versions prior to 22.1R2.

Recommendations

CERT-EU recommends applying the necessary patches and updates released by Juniper.

Workarounds

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

References

[1] https://supportportal.juniper.net/s/article/2022-10-Security-Bulletin-Junos-OS-Multiple-vulnerabilities-in-J-Web?language=en_US

[2] https://www.redpacketsecurity.com/juniper-networks-junos-os-command-execution-cve-2022-22241/