CERT-EU

Security Advisory 2024-038

Critical vulnerabilities in Junos OS and Junos OS Evolved

April 16, 2024 — v1.0

TLP:CLEAR

History:

- *16/04/2024 — v1.0 – Initial publication*

Summary

Multiple critical vulnerabilities have been identified in Juniper Networks Junos OS and Junos OS Evolved, primarily related to outdated cURL libraries [1]. These vulnerabilities could allow remote attackers to execute arbitrary code, cause denial of service, or leak sensitive information.

It is strongly advised to update affected systems to the latest versions to mitigate these risks.

Technical Details

The vulnerability **CVE-2023-38545**, with a CVSS score of 9.8, is due to a heap-based buffer overflow in SOCKS5 proxy handshake in curl that could allow remote attackers to execute arbitrary code.

The vulnerabilities **CVE-2023-23914** and **CVE-2023-23915**, respectively with CVSS scores of 9.1 and 6.5, are caused by HSTS mechanism failures, and would allow transmission of sensitive information over unencrypted channels under certain conditions.

The vulnerability **CVE-2020-8285**, with a CVSS score of 7.5, is due to improper certificate revocation checks.

The vulnerability **CVE-2020-8286**, with a CVSS score of 7.5, is due to improper handling of network responses would cause denial of service conditions.

The vulnerabilities **CVE-2018-1000120** and **CVE-2018-1000122**, respectively with CVSS scores of 9.8 and 9.1, are older buffer overflow and buffer over-read vulnerabilities affecting older versions of curl, and could cause denial of service, information leakage, or worse.

Affected Products

- **Junos OS**: All versions before 23.4R1-S1, 23.4R2
- **Junos OS Evolved**: All versions before 21.4R3-S4-EVO, from 22.1-EVO before 22.1R3-S4-EVO, from 22.3-EVO before 22.3R3-S1-EVO, and from 22.4-EVO before 22.4R2-S1-EVO.

Recommendations

It is strongly recommended updating affected devices to a fixed version.

References

[1] https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Multiple-cURL-vulnerabilities-resolved?language=en_US