Security Advisory 2023-079

Juniper Networks Junos OS Multiple Vulnerabilities

October 14, 2023 — v1.0

TLP:CLEAR

History:

- *14/10/2023 — v1.0 – Initial publication*

Summary

On October 14, 2023, Juniper Networks announced patches for more than 30 vulnerabilities in Junos OS and Junos OS Evolved, including nine high-severity flaws. The most severe vulnerability, tracked as **CVE-2023-44194** with a CVSS score of 8.4 out of 10, allows an unauthenticated attacker with local access to create a backdoor with root privileges due to incorrect default permissions in a certain system directory.

It is recommended applying updates as soon as possible.

Technical Details

Various vulnerabilities were addressed in this patch release, including:

- **CVE-2023-44194**: This vulnerability, with a CVSS score of 8.4 out of 10, is due to an incorrect default permissions bug that could allow an unauthenticated local attacker to create a backdoor with root privileges.
- **CVE-2023-44186**: This vulnerability, with a CVSS score of 7.5 out of 10, allows an attacker to send a BGP update message with an `AS PATH` containing a large number of 4-byte ASes, leading to a Denial of Service (DoS)

Affected Products

- Junos OS and Junos OS Evolved versions 20.4, 21.1, 21.2, 21.3, 21.4, 22.1, 22.2, 22.3, 22.4, 23.1, 23.2, and 23.3.

Recommendations

CERT-EU recommends updating affected devices to the latest versions as soon as possible.

Workaround

CVE-2023-44186

It is possible to limit the `AS PATH` length to mitigate this vulnerability.

```
Below is an example configuration to limit AS PATH to 30 entries:
set groups BASE-POLICY policy-options policy-statement MaxAS-Limit-30 term more-than-30 from
  protocol bgp
set groups BASE-POLICY policy-options policy-statement MaxAS-Limit-30 term more-than-30 from
  as-path 31as
set groups BASE-POLICY policy-options policy-statement MaxAS-Limit-30 term more-than-30 then
  reject
set groups BASE-POLICY policy-options policy-statement MaxAS-Limit-30 then accept
set groups BASE-POLICY policy-options policy-statement Customer-IN term MaxAS-Limit from policy
   MaxAS-Limit-30
set groups BASE-BGP protocols bgp group <*-CUSTOMER> import Customer-IN
set groups BASE-PREFIX-LISTS policy-options as-path 31as ".{31,}"
```

References

[1] https://www.securityweek.com/juniper-networks-patches-over-30-vulnerabilities-in-junos-os