October 12, 2023

Overall Rating - High

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

On October 11, 2023, Juniper published a security advisory to address vulnerabilities in multiple products.

The Cyber Centre encourages users and administrators to review the provided web link and apply the necessary updates.

Technical Details

An Improper Handling of Exceptional Conditions vulnerability in AS PATH processing of Juniper Networks Junos OS and Junos OS Evolved 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). Continued receipt and processing of these BGP updates will create a sustained Denial of Service (DoS) condition.

This issue is hit when the router has Non-Stop Routing (NSR) enabled, has a non-4-byte-AS capable BGP neighbor, receives a BGP update message with a prefix that includes a long AS PATH containing large number of 4-byte ASes, and has to advertise the prefix towards the non-4-byte-AS capable BGP neighbor.

This issue affects:

Juniper Networks Junos OS:

- All versions prior to 20.4R3-S8;
- 21.1 versions 21.1R1 and later;
- 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-S4;
- 22.2 versions prior to 22.2R3-S2;
- 22.3 versions prior to 22.3R2-S2, 22.3R3-S1;
- 22.4 versions prior to 22.4R2-S1, 22.4R3;
- 23.2 versions prior to 23.2R2.

Juniper Networks Junos OS Evolved

- All versions prior to 20.4R3-S8-EVO;
- 21.1 versions 21.1R1-EVO and later;
- 21.2 versions prior to 21.2R3-S6-EVO;
- 21.3 versions prior to 21.3R3-S5-EVO;
- 21.4 versions prior to 21.4R3-S5-EVO;
- 22.1 versions prior to 22.1R3-S4-EVO;
- 22.2 versions prior to 22.2R3-S2-EVO;
- 22.3 versions prior to 22.3R2-S2-EVO, 22.3R3-S1-EVO;
- 22.4 versions prior to 22.4R2-S1-EVO, 22.4R3-EVO;
- 23.2 versions prior to 23.2R2-EVO.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **high** risk. A software update exists to address this risk.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-44186, CVE-2023-44182, CVE-2023-44197, CVE-2023-44199, CVE-2023-44181, CVE-2023-44191, CVE-2023-44192, CVE-2023-44175, CVE-2023-44194, CVE-2023-44185,

- Juniper Networks Security Advisories

Please note that we will be transitioning to a new site on August 31, 2023, where we will post the vulnerability reports.

You will be able to find all the reports that we have published as well as all future reports here: Cybersecurity Alerts