Overall rating: High

BRITISH
COLUMBIA

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware Juniper Networks published a Security Advisory to address a vulnerability in the following products:

- Juniper Networks Junos OS – multiple versions
- Juniper Networks Junos OS Evolved – multiple versions

Technical Details

An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS).

When a BGP update message is received over an established BGP session, and that message contains a specific, optional transitive attribute, this session will be torn down with an update message error. This issue cannot propagate beyond an affected system as the processing error occurs as soon as the update is received. This issue is exploitable remotely as the respective attribute can propagate through unaffected systems and intermediate AS (if any).

Continuous receipt of a BGP update containing this attribute will create a sustained Denial of Service (DoS) condition.

Some customers have experienced these BGP session flaps which prompted Juniper SIRT to release this advisory out of cycle before fixed releases are widely available as there is an effective workaround.

This vulnerability is rated as a **High** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

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

References

- CVE-2023-0026
- Juniper Networks Security Advisory - JSA71542
- Juniper Networks Security Advisories