2022-07 Security Bulletin: Junos OS: RIB and PFEs can get out of sync due to a memory leak caused by interface flaps or route churn (CVE-2022-22209)

Article ID JSA69713 **Created** 2022-07-13

Last Updated 2022-07-13

Product Affected

This issue affects Junos OS 21.2, 21.3, 21.4.

Severity	Severity Assessment (CVSS) Score
High	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Problem

A Missing Release of Memory after Effective Lifetime vulnerability in the kernel of Juniper Networks Junos OS allows an unauthenticated network based attacker to cause a Denial of Service (DoS).

On all Junos platforms, the Kernel Routing Table (KRT) queue can get stuck due to a memory leak triggered by interface flaps or route churn leading to RIB and PFEs getting out of sync. The memory leak causes RTNEXTHOP/route and next-hop memory pressure issue and the KRT queue will eventually get stuck with the error- 'ENOMEM -- Cannot allocate memory'. The out-of-sync state between RIB and FIB can be seen with the "show route" and "show route forwarding-table" command. This issue will lead to failures for adding new routes.

The KRT queue status can be checked using the CLI command '`show krt queue`':

```
user@host > show krt state
High-priority add queue: 1 queued
ADD nhtype Router index 0 (31212)
error 'ENOMEM -- Cannot allocate memory'
kqp '0x8ad5e40'
```

The following messages will be observed in /var/log/messages, which indicate high memory for routes/nexthops:

```
host rpd[16279]: RPD_RT_HWM_NOTICE: New RIB highwatermark for routes: 266 [2022-03-
04 05:06:07]
host rpd[16279]: RPD_KRT_Q_RETRIES: nexthop ADD: Cannot allocate memory
host rpd[16279]: RPD_KRT_Q_RETRIES: nexthop ADD: Cannot allocate memory
host kernel: rts_veto_net_delayed_unref_limit: Route/nexthop memory is sever
pressure. User Application to perform recovery actions. O p 8 err 12, rtsm_i
msg type 10, veto simulation: 0.
host kernel: rts_veto_net_delayed_unref_limit: Memory usage of M_RTNEXTHOP t
```

```
(806321208) Max size possible for M_RTNEXTHOP type = (689432176) Current del
unref = (0), Max delayed unref on this platform = (120000) Current delayed we
unref = (0) Max delayed weight unref on this platform = (400000) curproc = rpd.
```

This issue affects:
Juniper Networks Junos OS

- 21.2 versions prior to 21.2R3;
- 21.3 versions prior to 21.3R2-S1, 21.3R3;
- 21.4 versions prior to 21.4R1-S2, 21.4R2;

This issue does not affect Juniper Networks Junos OS versions prior to 21.2R1.

This issue was seen during production usage.
This issue has been assigned CVE-2022-22209.

Solution

The following software releases have been updated to resolve this specific issue: 21.2R3, 21.3R2-S1, 21.3R3, 21.4R1-S2, 21.4R2, 22.1R1, and all subsequent releases.

Note: Only those releases listed in the PROBLEM section above are affected. This fix has also been proactively committed into other releases that are not vulnerable to this issue.

Note: Juniper SIRT's policy is not to evaluate releases which are beyond End of Engineering (EOE) or End of Life (EOL).

This issue is being tracked as 1642172.

Workaround

There are no known workarounds for this issue.

Modification History

```
2022-07-13: Initial publication
```

Related Information

- KB16613: Overview of the Juniper Networks SIRT Quarterly Security Bulletin Publication Process
- KB16765: In which releases are vulnerabilities fixed?
- KB16446: Common Vulnerability Scoring System (CVSS) and Juniper's Security Advisories
- Report a Security Vulnerability - How to Contact the Juniper Networks Security Incident Response Team

AFFECTED PRODUCT SERIES / FEATURES

People also viewed