2021-01 Security Bulletin: Junos OS: EX Series and QFX Series: Memory leak issue processing specific DHCP packets (CVE-2021-0217)

Article ID JSA11107 **Created** 2020-12-30 **Last Updated** 2021-01-22

Product Affected

This issue affects Junos OS 17.4R3, 18.1R3, 18.2R3, 18.3R3, 18.4R2, 18.4R3, 19.1, 19.2, 19.3, 19.4, 20.1, 20.2.
Affected platforms: EX Series, QFX Series.

Severity	Severity Assessment (CVSS) Score
High	7.4 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H)

Problem

A vulnerability in processing of certain DHCP packets from adjacent clients on EX Series and QFX Series switches running Juniper Networks Junos OS with DHCP local/relay server configured may lead to exhaustion of DMA memory causing a Denial of Service (DoS). Over time, exploitation of this vulnerability may cause traffic to stop being forwarded, or to crashing of the fxpc process.
When Packet DMA heap utilization reaches 99%, the system will become unstable. Packet DMA heap utilization can be monitored through the following command:

```
user@junos# request pfe execute target fpc0 timeout 30 command "show heap"
ID Base Total(b) Free(b) Used(b) % Name
-- ---------- ---------- ---------- ---------- --- ----------
0 213301a8 536870488 387228840 149641648 27 Kernel
1 91800000 8388608 3735120 4653488 55 DMA
2 92000000 75497472 74452192 1045280 1 PKT DMA DESC
3 d330000 335544320 257091400 78452920 23 Bcm_sdk
4 96800000 184549376 2408 184546968 99 Packet DMA
5 903fffe0 20971504 20971504 0 0 Blob
```

An indication of the issue occurring may be observed through the following log messages:

```
Dec 10 08:07:00.124 2020 hostname fpc0 brcm_pkt_buf_alloc:523 (buf alloc) failed allocating packet buffer
Dec 10 08:07:00.126 2020 hostname fpc0 (buf alloc) failed allocating packet buffer
Dec 10 08:07:00.128 2020 hostname fpc0 brcm_pkt_buf_alloc:523 (buf alloc) failed allocating packet buffer
Dec 10 08:07:00.130 2020 hostnameC fpc0 (buf alloc) failed allocating packet buffer
```

This issue affects Juniper Networks Junos OS on EX Series and QFX Series:

- 17.4R3 versions prior to 17.4R3-S3;
- 18.1R3 versions between 18.1R3-S6 and 18.1R3-S11;
- 18.2R3 versions prior to 18.2R3-S6;
- 18.3R3 versions prior to 18.3R3-S4;
- 18.4R2 versions prior to 18.4R2-S5;
- 18.4R3 versions prior to 18.4R3-S6;
- 19.1 versions between 19.1R2 and 19.1R3-S3;
- 19.2 versions prior to 19.2R3-S1;
- 19.3 versions prior to 19.3R2-S5, 19.3R3;
- 19.4 versions prior to 19.4R2-S2, 19.4R3;
- 20.1 versions prior to 20.1R2;
- 20.2 versions prior to 20.2R1-S2, 20.2R2.

Junos OS versions prior to 17.4R3 are unaffected by this vulnerability.

The following configuration snippet enables the DHCP relay forwarding option:

```
[forwarding-options dhcp-relay]
```

The following configuration provides an example of enabling DHCP local server:

```
[system services dhcp]
```

Juniper SIRT is not aware of any malicious exploitation of this vulnerability.
This issue was seen during production usage.
This issue has been assigned CVE-2021-0217 .

Solution

The following software releases have been updated to resolve this specific issue: Junos OS 17.4R3-S3, 18.1R3-S11, 18.2R3-S6, 18.3R3-S4, 18.4R2-S5, 18.4R3-S6, 19.1R1-S6, 19.1R3-S3, 19.2R3-S1, 19.3R2-S5, 19.3R3, 19.4R2-S2, 19.4R3, 20.1R2, 20.2R1-S2, 20.2R2, 20.3R1, and all subsequent releases.
This issue is being tracked as 1514145 .

Software releases or updates are available for download at https://www.juniper.net/support/downloads/ .

Workaround

There are no available workarounds for this issue.

Modification History

```
2021-01-13: Initial Publication.
2021-01-15: Removed redundant 18.4R2-S7 fixed release from SOLUTION field.
2021-01-22: Added sample configuration for DHCP local server.
```

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
- CVE-2021-0217 at cve.mitre.org

AFFECTED PRODUCT SERIES / FEATURES

People also viewed