2022-10 Security Bulletin: Junos OS: QFX10000 Series: In IP/MPLS PHP node scenarios upon receipt of certain crafted packets multiple interfaces in LAG configurations may detach. (CVE-2022-22223)

Article ID JSA69873 **Created** 2022-10-12

Last Updated 2022-10-12

Product Affected

This issue affects all versions of Junos OS. Affected platforms: QFX10000 Series.

Severity

Medium

Severity Assessment (CVSS) Score

6.5 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Problem

On QFX10000 Series devices using Juniper Networks Junos OS when configured as transit IP/MPLS penultimate hop popping (PHP) nodes with link aggregation group (LAG) interfaces, an Improper Validation of Specified Index, Position, or Offset in Input weakness allows an attacker sending certain IP packets to cause multiple interfaces in the LAG to detach causing a Denial of Service (DoS) condition.

Continued receipt and processing of these packets will sustain the Denial of Service.

This issue affects IPv4 and IPv6 packets. Packets of either type can cause and sustain the DoS event.

These packets can be destined to the device or be transit packets.

On devices such as the QFX10008 with line cards, line cards can be restarted to restore service. On devices such as the QFX10002 you can restart the PFE service, or reboot device to restore service.This issue affects:
Juniper Networks Junos OS on QFX10000 Series:

- All versions prior to 15.1R7-S11;
- 18.4 versions prior to 18.4R2-S10, 18.4R3-S10;
- 19.1 versions prior to 19.1R3-S8;
- 19.2 versions prior to 19.2R3-S4;
- 19.3 versions prior to 19.3R3-S5;
- 19.4 versions prior to 19.4R2-S6, 19.4R3-S7;
- 20.1 versions prior to 20.1R3-S3;
- 20.2 versions prior to 20.2R3-S3;
- 20.3 versions prior to 20.3R3-S2;
- 20.4 versions prior to 20.4R3-S4;

- 21.1 versions prior to 21.1R3;
- 21.2 versions prior to 21.2R3-S3;
- 21.3 versions prior to 21.3R3-S1.

An indicator of compromise may be seen by issuing the command:

```
 request pfe execute target fpc0 command "show jspec pechip[3] registers ps l2_node 10" timeout 0 | refresh 1 | no-more
```

and reviewing for backpressured output; for example:

```
  GOT: 0x220702a8  pe.ps.l2_node[10].pkt_cnt              00000076
  GOT: 0x220702b4  pe.ps.l2_node[10].backpressured        00000002 <<<< STICKS HERE
```

and requesting detail on the pepic wanio:

```
request pfe execute target fpc0 command "show pepic 0 wanio-info" timeout 0 | no-more | match xe-0/0/0:2
GOT:  3   xe-0/0/0:2      10       6          3      0        1     10    189
       10   0x6321b088  <<< LOOK HERE
```

as well as looking for tail drops looking at the interface queue, for example:

```
  show interfaces queue xe-0/0/0:2
```

resulting in:

```
  Transmitted:
  Total-dropped packets:               1094137                        0 pps << LOOK
HERE
```

The following minimal configuration is required to be potentially impacted by this issue:

```
[interfaces <interface> unit <unit> family inet address <address/mask>]
[interfaces <interface> unit <unit> family mpls]
[protocols rsvp interface <interface>]
[protocols mpls interface <interface>]
[protocols ospf area <area> interface <interface>]
```

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-2022-22223.

Solution

The following software releases have been updated to resolve this specific issue: 15.1R7-S11, 18.4R2-S10, 18.4R3-S10, 19.1R3-S8, 19.2R3-S4, 19.3R3-S5, 19.4R2-S6, 19.4R3-S7, 20.1R3-S3, 20.2R3-S3, 20.3R3-S2, 20.4R3-S4, 21.1R3, 21.2R3-S3, 21.3R3-S1 21.4R1, and all subsequent releases.
This issue is being tracked as PR 1618728 which is visible on the Customer Support website.
Note: Juniper SIRT's policy is not to evaluate releases which are beyond End of Engineering (EOE) or End of Life (EOL).

IMPLEMENTATION:

Software Releases, patches and updates are available at https://support.juniper.net/support/downloads/.

Workaround

Customers can apply the following PFE VTY commands as a workaround until a fixed release can be taken:

```
bringup jspec write pechip[0] register egp main init_params 36 00000068
bringup jspec write pechip[1] register egp main init_params 36 00000068
bringup jspec write pechip[2] register egp main init_params 36 00000068
bringup jspec write pechip[3] register egp main init_params 36 00000068
bringup jspec write pechip[4] register egp main init_params 36 00000068
bringup jspec write pechip[5] register egp main init_params 36 00000068
```

This workaround must be reapplied upon any reboot.

Modification History

2022-10-12: 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
- CVE-2022-22223 at cve.mitre.org

AFFECTED PRODUCT SERIES / FEATURES

People also viewed