2022-07 Security Bulletin: Junos OS: PTX Series: FPCs may restart unexpectedly upon receipt of specific MPLS packets with certain multi-unit interface configurations (CVE-2022-22202)

Article ID JSA69706 **Created** 2022-07-13

Last Updated 2022-07-14

Product Affected

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

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

Problem

An Improper Handling of Exceptional Conditions vulnerability on specific PTX Series devices, including the PTX1000, PTX3000 (NextGen), PTX5000, PTX10002-60C, PTX10008, and PTX10016 Series, in Juniper Networks Junos OS allows an unauthenticated MPLS-based attacker to cause a Denial of Service (DoS) by triggering the dcpfe process to crash and FPC to restart. On affected PTX Series devices, processing specific MPLS packets received on an interface with multiple units configured may cause FPC to restart unexpectedly. Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition.

This issue only affects PTX Series devices utilizing specific FPCs found on PTX1000, PTX3000 (NextGen), PTX5000, PTX10002-60C, PTX10008, and PTX10016 Series devices, only if multiple units are configured on the ingress interface, and at least one unit has 'family mpls' *not* configured. See the configuration sample below for more information.

No other platforms are affected by this vulnerability.

This issue affects Juniper Networks Junos OS on PTX Series:

- All versions prior to 19.1R3-S9;
- 19.2 versions prior to 19.2R3-S6;
- 19.3 versions prior to 19.3R3-S6;
- 19.4 versions prior to 19.4R3-S8;
- 20.1 versions prior to 20.1R3-S4;
- 20.2 versions prior to 20.2R3-S5;
- 20.3 versions prior to 20.3R3-S4;
- 20.4 versions prior to 20.4R3-S4;
- 21.1 versions prior to 21.1R3-S2;
- 21.2 versions prior to 21.2R3-S1;
- 21.3 versions prior to 21.3R3;

- 21.4 versions prior to 21.4R2;
- 22.1 versions prior to 22.1R2.

The FPC crash only occurs if specific MPLS packets are received on an interface with multiple units configured and at least one unit has 'family mpls' not configured. Also, the first unit with family mpls configured is not the lowest numerical unit on that interface.

A sample vulnerable configuration utilizing multiple units on an interface with MPLS enabled is shown below:

```
set interfaces et-0/0/37:2 vlan-tagging
set interfaces et-0/0/37:2 unit 0 vlan-id 0 <<< 'family mpls' not configured
set interfaces et-0/0/37:2 unit 5 vlan-id 3000
set interfaces et-0/0/37:2 unit 5 family inet6 address fe80::ce1/64
set interfaces et-0/0/37:2 unit 7 vlan-id 3032
set interfaces et-0/0/37:2 unit 7 family inet address 169.254.101.23/31
set interfaces et-0/0/37:2 unit 7 family inet6
set interfaces et-0/0/37:2 unit 7 family mpls <<< 'family' mpls configured, but not
the lowest unit number
set interfaces et-0/0/37:2 unit 10 vlan-id 10
set interfaces et-0/0/37:2 unit 10 family inet address 192.168.10.1/24
set interfaces et-0/0/37:2 unit 10 family iso
set interfaces et-0/0/37:2 unit 10 family mpls
...
```

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-2022-22202.

Solution

The following software releases have been updated to resolve this specific issue: Junos OS 19.1R3-S9, 19.2R3-S6, 19.3R3-S6, 19.4R3-S8, 20.1R3-S4, 20.2R3-S5, 20.3R3-S4, 20.4R3-S4, 21.1R3-S2, 21.2R3-S1, 21.3R3, 21.4R2, 22.1R2, 22.2R1, and all subsequent releases.

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 1649586.

Workaround

The FPC crash only occurs if specific MPLS packets are received on an interface with multiple units configured and at least one unit has family mpls not configured. Also, the first unit with family mpls configured is not the lowest numerical unit on that interface.

A viable config-based workaround would be to reorder the unit numbers on core-facing interfaces to ensure the numerically lowest unit has '`family mpls`' configured.

Modification History

```
2022-07-13: Initial publication
2022-07-14: Clarified that a dcpfe process crash leads to the FPC restart
```

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