2022-10 Security Bulletin: Junos OS: MX Series: An FPC crash might be seen due to mac-moves within the same bridge domain (CVE-2022-22249)

Article ID JSA69906 **Created** 2022-10-12

Last Updated 2022-10-12

Product Affected

This issue affects Junos OS all versions prior to 15.1R7-S13, 16.1R1 and all subsequent versions prior to 19.1R3-S9, 19.2, 19.3, 19.4, 20.2, 20.3, 20.4, 21.1, 21.2, 21.3. Affected platforms: MX 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 Control of a Resource Through its Lifetime vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX Series allows an unauthenticated adjacent attacker to cause a Denial of Service (DoS).
When there is a continuous mac move a memory corruption causes one or more FPCs to crash and reboot. These MAC moves can be between two local interfaces or between core/EVPN and local interface.
The below error logs can be seen in PFE syslog when this issue happens:

```
xss_event_handler(1071): EA[0:0]_PPE 46.xss[0] ADDR Error.
ppe_error_interrupt(4298): EA[0:0]_PPE 46 Errors sync xtxn error
xss_event_handler(1071): EA[0:0]_PPE 1.xss[0] ADDR Error.
ppe_error_interrupt(4298): EA[0:0]_PPE 1 Errors sync xtxn error
xss_event_handler(1071): EA[0:0]_PPE 2.xss[0] ADDR Error.
```

This issue affects Juniper Networks Junos OS on MX Series:

- All versions prior to 15.1R7-S13;
- 19.1 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 19.4R2-S7, 19.4R3-S8;
- 20.1 version 20.1R1 and later versions;
- 20.2 versions prior to 20.2R3-S5;
- 20.3 versions prior to 20.3R3-S5;
- 20.4 versions prior to 20.4R3-S2;
- 21.1 versions prior to 21.1R3;
- 21.2 versions prior to 21.2R3;
- 21.3 versions prior to 21.3R2.

To be exposed to this vulnerability the device would need to have a minimal bridge domain configuration v
interfaces:

```
[ bridge-domains <bridge-name> interface <interface-1> ]
[ bridge-domains <bridge-name> interface <interface-2> ]
```

or at least one local interface as above and EVPN MPLS as follows:

```
[protocols bgp group <group-name> family evpn]
```

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-2022-22249.

Solution

The following software releases have been updated to resolve this specific issue: 15.1R7-S13, 19.1R3-S9, 19.2R3-S6, 19.3R3-S6, 19.4R2-S7, 19.4R3-S8, 20.2R3-S5, 20.3R3-S5, 20.4R3-S2, 21.1R3, 21.2R3, 21.3R2, 21.4R1, and all subsequent releases.
This issue is being tracked as PR 1607767 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

There are no known workarounds for this issue.

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-2022-22249 at cve.mitre.org

AFFECTED PRODUCT SERIES / FEATURES