2021-10 Security Bulletin: Junos OS: MX Series: MPC 7/8/9/10/11 cards with MAP-E: PFE halts when an attacker sends malformed IPv4 or IPv6 traffic inside the MAP-E tunnel. (CVE-2021-31379)

Article ID JSA11247 **Created** 2021-09-28 **Last Updated** 2021-10-13

Product Affected

This issue affects Junos OS 17.2, 17.3, 17.4, 18.1, 18.2, 18.3, 18.4, 19.1, 19.2, 19.3. Affected platforms: MX Series

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

An Incorrect Behavior Order vulnerability in the MAP-E automatic tunneling mechanism of Juniper Networks Junos OS allows an attacker to send certain malformed IPv4 or IPv6 packets to cause a Denial of Service (DoS) to the PFE on the device which is disabled as a result of the processing of these packets.
Continued receipt and processing of these malformed IPv4 or IPv6 packets will create a sustained Denial of Service (DoS) condition.
This issue only affects MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards.
An indicator of compromise is the output:

```
FPC ["FPC ID" # e.g. "0"]
PFE #{PFE ID # e.g. "1"]
: Fabric Disabled
```

Example:

```
FPC 0
PFE #1
: Fabric Disabled
```

when using the command:

```
show chassis fabric fpcs
```

An example of a healthy result of the command use would be:

```
user@device-re1> show chassis fabric fpcs
Fabric management FPC state:
FPC 0
PFE #0
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled
```

This issue affects:
Juniper Networks Junos OS on MX Series with MPC 7/8/9/10/11 cards, when MAP-E IP reassembly is enabled on these cards.

- 17.2 version 17.2R1 and later versions;
- 17.3 versions prior to 17.3R3-S9;
- 17.4 versions prior to 17.4R2-S12, 17.4R3-S3;
- 18.1 versions prior to 18.1R3-S11;
- 18.2 versions prior to 18.2R2-S6, 18.2R3-S3;
- 18.3 versions prior to 18.3R2-S4, 18.3R3-S1;
- 18.4 versions prior to 18.4R1-S8, 18.4R2-S5, 18.4R3;
- 19.1 versions prior to 19.1R1-S6, 19.1R2-S2, 19.1R3;
- 19.2 versions prior to 19.2R1-S5, 19.2R2;
- 19.3 versions prior to 19.3R2-S5, 19.3R3.

This issue does not affect Juniper Networks Junos OS versions prior to 17.2R1.
The following minimal configuration is necessary:

```
[chassis fpc <fpc-number> pic <pic-number> inline-services bandwidth <bandwidth> ]
[interfaces <si-interface-name> unit <inside-logical-unit> family inet]
[interfaces <si-interface-name> unit <inside-logical-unit> family inet6]
[interfaces <si-interface-name> unit <inside-logical-unit> service-domain inside]
[interfaces <si-interface-name> unit <outside-logical-unit> family inet]
[interfaces <si-interface-name> unit <outside-logical-unit> family inet6]
[interfaces <si-interface-name> unit <outside-logical-unit> service-domain outside]
[services softwire softwire-concentrator map-e <mape-instance-name> version03]
[services softwire softwire-concentrator map-e <mape-instance-name> softwire-address <IPv6-Address> ]
[services softwire softwire-concentrator map-e <mape-instance-name> ipv4-prefix <IPv4-Prefix> mape-prefix <IPv6-Prefix> ]
[services softwire softwire-concentrator map-e <mape-instance-name> ea-bits-len <0..48>]
[services softwire softwire-concentrator map-e <mape-instance-name> psid-off[set <0..16>]
[services softwire softwire-concentrator map-e <mape-instance-name> psid-length <0..16>]
[services softwire softwire-concentrator map-e <mape-instance-name> mtu-ipv6 <1280..9192>]
[services softwire softwire-concentrator map-e <mape-instance-name> v4-reassembly]
[services softwire rule <mape-rule-name> match-direction input term <term-name> then map-e <mape-instance-name> ]
[services service-set <service-set-name> softwire-rules <mape-rule-name> ]
[services service-set <service-set-name> next-hop-service inside-service-interface <si-interface-name.inside-logical-unit> outside-service-interface <si-interface-name.outside-logical-unit> ]
```

Juniper SIRT is not aware of any malicious exploitation of this vulnerability.
This issue was found during internal product security testing or research.
This issue has been assigned CVE-2021-31379 .

Solution

The following software releases have been updated to resolve this specific issue: 17.3R3-S9, 17.4R2-S12, 17.4R3-S3, 18.1R3-S11, 18.2R2-S6, 18.2R3-S3, 18.3R2-S4, 18.3R3-S1, 18.4R1-S8, 18.4R2-S5, 18.4R3, 19.1R1-S6, 19.1R2-S2, 19.1R3, 19.2R1-S5, 19.2R2, 19.3R2-S5, 19.3R3, 19.4R1, and all subsequent releases.
This issue is being tracked as 1468454 .
Software releases or updates are available for download at https://support.juniper.net/support/downloads/

Workaround

To work around this issue customers can either:
1. Disable Mapping of Address and port - Encapsulation (MAP-E) as an inline service on MX Series routers that use MPC and MIC interfaces.
or
2. Determine where the MAP-E v4 or v6 reassembly exists, review the following hierarchies and disable the "v4-reassembly;" and "v6-reassembly;" options where they exist:

```
[services softwire softwire-concentrator]
```

```
[services softwires softwire-types]
[security softwires]
```

and the following syntaxes:

```
map-e name {
v4-reassembly; <<<<< DISABLE the v4-reassembly option.
v6-reassembly; <<<<< DISABLE the v6-reassembly option.
}
```

Modification History

```
2021-10-13: 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 Vulnerability - How to Contact the Juniper Networks Security Incident Response Team
- CVE-2021-31379 at cve.mitre.org
- Configuring Mapping of Address and Port with Encapsulation (MAP-E)

AFFECTED PRODUCT SERIES / FEATURES

People also viewed