# 2021-01 Security Bulletin: Junos OS: EX Series, QFX Series, MX Series, SRX Branch Series: Memory leak in packet forwarding engine due to 802.1X authenticator port interface flaps (CVE-2021-0215)

**Article ID** JSA11105 **Created** 2020-12-31 **Last Updated** 2021-03-16

**Product Affected**

This issue affects Junos OS 14.1X53, 15.1X49, 15.1X53, 16.1, 17.2, 17.3, 17.4, 18.1, 18.2, 18.3, 18.4, 19.1, 19.2, 19.3, 19.4. Affected platforms: EX Series, QFX Series, MX Series, SRX Branch 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**

On Juniper Networks Junos EX series, QFX Series, MX Series, and SRX branch series devices, a memory leak occurs every time the 802.1X authenticator port interface flaps which can lead to other processes, such as the pfex process, responsible for packet forwarding, to crash and restart.
An administrator can use the following CLI command to monitor the status of memory consumption:

```
user@device> show task memory detail
```

Please refer to https://kb.juniper.net/KB31522 for details.
This issue affects Juniper Networks Junos OS:
14.1X53 versions prior to 14.1X53-D54;
15.1X49 versions prior to 15.1X49-D240 ;
15.1X53 versions prior to 15.1X53-D593;
16.1 versions prior to 16.1R7-S8;
17.2 versions prior to 17.2R3-S4;
17.3 versions prior to 17.3R3-S8;
17.4 versions prior to 17.4R2-S11, 17.4R3-S2;
18.1 versions prior to 18.1R3-S10 ;
18.2 versions prior to 18.2R2-S7, 18.2R3-S3;
18.3 versions prior to 18.3R2-S4, 18.3R3-S2;
18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18.4R3-S2;
19.1 versions prior to 19.1R1-S5, 19.1R2-S2, 19.1R3;
19.2 versions prior to 19.2R1-S5, 19.2R2;
19.3 versions prior to 19.3R2-S3, 19.3R3;
19.4 versions prior to 19.4R1-S2, 19.4R2.
This issue does not affect Juniper Networks Junos OS 12.3, 15.1.

This issue may occur when the device is configured as 802.1X authenticator port and the interface flaps.
Minimum configuration stanza required related to this issue is the following:

```
[dot1x]
```

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-2021-0215 .

**Solution**

The following software releases have been updated to resolve this specific issue: 14.1X53-D54, 15.1X49-D240, 15.1X53-D593, 16.1R7-S8, 17.2R3-S4, 17.3R3-S8, 17.4R2-S11, 17.4R3-S2, 18.1R3-S10, 18.2R2-S7, 18.2R3-S3, 18.3R2-S4, 18.3R3-S2, 18.4R1-S7, 18.4R2-S4, 18.4R3-S2, 19.1R1-S5, 19.1R2-S2, 19.1R3, 19.2R1-S5, 19.2R2, 19.3R2-S3, 19.3R3, 19.4R1-S2, 19.4R2, 20.1R1, and all subsequent releases.
This issue is being tracked as 1480706 .
Software releases or updates are available for download at https://www.juniper.net/support/downloads/ .

**Workaround**

There are no viable workarounds for this issue.

**Modification History**

2021-01-13: Initial Publication.
2021-03-02: MX series added to affected products.

**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-2021-0215 at cve.mitre.org
- How to verify the memory limitation for each process

AFFECTED PRODUCT SERIES / FEATURES

People also viewed