2022-04 Security Bulletin: Junos OS: QFX5100/QFX5110/QFX5120/QFX5200/QFX5210/EX4600/EX4650 Series: When storm control profiling is enabled and a device is under an active storm, a Heap-based Buffer Overflow in the PFE will cause a device to hang.

Article ID JSA69497 **Created** 2022-04-13

Last Updated 2022-04-13

Product Affected

This issue affects Junos OS 20.2. Affected platforms: QFX5100/QFX5110/QFX5120/QFX5200/QFX5210/EX4600/EX4650 Series.

Severity

High

Severity Assessment (CVSS) Score

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

Problem

An Uncontrolled Memory Allocation vulnerability leading to a Heap-based Buffer Overflow in the packet forwarding engine (PFE) of Juniper Networks Junos OS allows a network-based unauthenticated attacker to flood the device with traffic leading to a Denial of Service (DoS). The device must be configured with storm control profiling limiting the number of unknown broadcast, multicast, or unicast traffic to be vulnerable to this issue.

This issue affects:
Juniper Networks Junos OS on QFX5100/QFX5110/QFX5120/QFX5200/QFX5210/EX4600/EX4650 Series;

- 20.2 version 20.2R1 and later versions prior to 20.2R2.

This issue does not affect:
Juniper Networks Junos OS versions prior to 20.2R1.

The following is an example of the configuration required to be impacted by this issue.
Please refer to your documentation for specific configuration guidance:

```
set interfaces xe-0/0/9:1 unit 0 family ethernet-switching interface-mode trunk
set interfaces xe-0/0/9:1 unit 0 family ethernet-switching vlan members 100
set interfaces xe-0/0/9:1 unit 0 family ethernet-switching storm-control sc
set forwarding-options storm-control-profiles sc all
set forwarding-options storm-control-profiles sc action-shutdown
set vlans vlan100 vlan-id 100
```

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-2022-22188.

Solution

The following software releases have been updated to resolve this specific issue: 20.2R2, 20.3R1, and all subsequent releases.
This issue is being tracked as PR 1525821 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://www.juniper.net/support/downloads/.

Workaround

There are no viable workarounds for this issue.

Modification History

- `2022-04-13: 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 Security Vulnerability - How to Contact the Juniper Networks Security Incident Response Team
- CVE-2022-22188 at cve.mitre.org

AFFECTED PRODUCT SERIES / FEATURES

People also viewed