2020-04 Security Bulletin: Junos OS: Kernel memory leak in virtual-memory due to interface flaps (CVE-2020-1625)

Article ID JSA11004 **Created** 2020-03-24 **Last Updated** 2020-04-08

Product Affected

This issue affects Junos OS 16.1, 17.1, 17.2, 17.2X75, 17.3, 17.4, 18.1, 18.2, 18.2X75, 18.3, 18.4, 19.1, 19.2.

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

The kernel memory usage represented as "temp" via 'show system virtual-memory' may constantly increase when Integrated Routing and Bridging (IRB) is configured with multiple underlay physical interfaces, and one interface flaps. This memory leak can affect running daemons (processes), leading to an extended Denial of Service (DoS) condition.

Usage of "temp" virtual memory, shown here by a constantly increasing value of outstanding Requests, can be monitored by executing the ' **show system virtual-memory** ' command as shown below:

```
user@junos> show system virtual-memory |match "fpc|type|temp"
fpc0:
--------------------------------------------------------------------------
Type InUse MemUse HighUse Requests Size(s)
temp 2023 431K - 10551 16,32,64,128,256,512,1024,2048,4096,65536,262144,1048576,2097152,4194304,8388608
fpc1:
--------------------------------------------------------------------------
Type InUse MemUse HighUse Requests Size(s)
temp 2020 431K - 6460 16,32,64,128,256,512,1024,2048,4096,65536,262144,1048576,2097152,4194304,8388608

user@junos> show system virtual-memory |match "fpc|type|temp"
fpc0:
--------------------------------------------------------------------------
Type InUse MemUse HighUse Requests Size(s)
temp 2023 431K - 16101 16,32,64,128,256,512,1024,2048,4096,65536,262144,1048576,2097152,4194304,8388608
fpc1:
--------------------------------------------------------------------------
Type InUse MemUse HighUse Requests Size(s)
temp 2020 431K - 6665 16,32,64,128,256,512,1024,2048,4096,65536,262144,1048576,2097152,4194304,8388608

user@junos> show system virtual-memory |match "fpc|type|temp"
fpc0:
--------------------------------------------------------------------------
Type InUse MemUse HighUse Requests Size(s)
temp 2023 431K - 21867 16,32,64,128,256,512,1024,2048,4096,65536,262144,1048576,2097152,4194304,8388608
fpc1:
--------------------------------------------------------------------------
Type InUse MemUse HighUse Requests Size(s)
temp 2020 431K - 6858 16,32,64,128,256,512,1024,2048,4096,65536,262144,1048576,2097152,4194304,8388608
```

This issue affects Juniper Networks Junos OS:

- 16.1 versions prior to 16.1R7-S6;
- 17.1 versions prior to 17.1R2-S11, 17.1R3-S1;
- 17.2 versions prior to 17.2R2-S8, 17.2R3-S3;
- 17.2X75 versions prior to 17.2X75-D44;
- 17.3 versions prior to 17.3R2-S5, 17.3R3-S6;
- 17.4 versions prior to 17.4R2-S5, 17.4R3;
- 18.1 versions prior to 18.1R3-S7;
- 18.2 versions prior to 18.2R2-S5, 18.2R3;
- 18.2X75 versions prior to 18.2X75-D33, 18.2X75-D411, 18.2X75-D420, 18.2X75-D60;
- 18.3 versions prior to 18.3R1-S5, 18.3R2-S3, 18.3R3;
- 18.4 versions prior to 18.4R2-S2, 18.4R3;
- 19.1 versions prior to 19.1R1-S3, 19.1R2;
- 19.2 versions prior to 19.2R1-S3, 19.2R2.

This issue does not affect Juniper Networks Junos OS 12.3 nor 15.1.

Minimum configuration required:

```
set interfaces irb
```

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-2020-1625 .

Solution

The following software releases have been updated to resolve this specific issue: 16.1R7-S6, 17.1R2-S11, 17.1R3-S1, 17.2R2-S8, 17.2R3-S3, 17.2X75-D44, 17.3R2-S5, 17.3R3-S6, 17.4R2-S5, 17.4R3, 18.1R3-S7, 18.2R2-S5, 18.2R3, 18.2X75-D33, 18.2X75-D411, 18.2X75-D420, 18.2X75-D60, 18.3R1-S5, 18.3R2-S3, 18.3R3, 18.4R2-S2, 18.4R3, 19.1R1-S3, 19.1R2, 19.2R1-S3, 19.2R2, 19.3R1, and all subsequent releases.
This issue is being tracked as 1407000 .

How to obtain fixed software:

Security vulnerabilities in Junos are fixed in the next available Maintenance Release of each supported Junos version. In some cases, a Maintenance Release is not planned to be available in an appropriate time-frame. For these cases, Service Releases are made available in order to be more timely. Security Advisory and Security Notices will indicate which Maintenance and Service Releases contain fixes for the issues described. **Upon request to JTAC** , customers will be provided download instructions for a Service Release. Although Juniper does not provide formal Release Note documentation for a Service Release, a list of "PRs fixed" can be provided on request.

Workaround

There are no viable workarounds for this issue.

Modification History

```
2020-04-08: 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-2020-1625: Junos OS: Kernel memory leak in virtual-memory due to interface flaps

AFFECTED PRODUCT SERIES / FEATURES

People also viewed