2022-07 Security Bulletin: Junos OS and Junos OS Evolved: /var/run/<pid>.env files are potentially not deleted during termination of a gRPC connection causing inode exhaustion (CVE-2022-22215)

Article ID JSA69719 **Created** 2022-07-13

Last Updated 2022-07-13

Product Affected

This issue affects all versions of Junos OS and Junos OS Evolved.

Severity	Severity Assessment (CVSS) Score
Medium	6.5 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

Problem

A Missing Release of File Descriptor or Handle after Effective Lifetime vulnerability in plugable authentication module (PAM) of Juniper Networks Junos OS and Junos OS Evolved allows a locally authenticated attacker with low privileges to cause a Denial of Service (DoS).

It is possible that after the termination of a gRPC connection the respective/var/run/<pid>.env file is not getting deleted which if occurring repeatedly can cause inode exhaustion.

Inode exhaustion can present itself in two different ways:
1. The following log message can be observed:

```
host kernel: pid <pid> (<process>), uid <uid> inumber <number> on /.mount/var: out of inodes
```

which by itself is a clear indication.
2. The following log message can be observed:

```
host <process>[<pid>]: ... : No space left on device
```

which is not deterministic and just a representation of a write error which could have several reasons. So the following check needs to be done:

```
user@host> show system storage no-forwarding
Filesystem Size Used Avail Capacity Mounted on
/dev/ada1p1 475M 300M 137M 69% /.mount/var
```

which indicates that the write error is not actually due to a lack of disk space.
If either 1. or 2. has been confirmed, then the output of:
user@host> file list /var/run/*.env | count
need to be checked and if it indicates a high (>10000) number of files the system has been affected by this

This issue affects:
Juniper Networks Junos OS

- All versions prior to 19.1R3-S8;
- 19.2 versions prior to 19.2R3-S6;
- 19.3 versions prior to 19.3R3-S5;
- 19.4 versions prior to 19.4R2-S6, 19.4R3-S7;
- 20.1 version 20.1R1 and later versions;
- 20.2 versions prior to 20.2R3-S5;
- 20.3 versions prior to 20.3R3-S4;
- 20.4 versions prior to 20.4R3;
- 21.1 versions prior to 21.1R3;
- 21.2 versions prior to 21.2R2.

Juniper Networks Junos OS Evolved

- All versions prior to 20.4R3-EVO;
- 21.1 versions prior to 21.1R3-S1-EVO;
- 21.2 versions prior to 21.2R1-S1-EVO, 21.2R2-EVO.

To be affected by this issue the system needs to be configured for gRPC:

```
[ system services extension-service request-response grpc ]
```

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-2022-22215.

Solution

The following software releases have been updated to resolve this specific issue:

Junos OS: 19.1R3-S8, 19.2R3-S6, 19.3R3-S5, 19.4R2-S6, 19.4R3-S7, 20.2R3-S5, 20.3R3-S4, 20.4R3, 21.1R3, 21.2R2, 21.3R1, and all subsequent releases;

Junos OS Evolved: 20.4R3-EVO, 21.1R3-S1-EVO, 21.2R1-S1-EVO, 21.2R2-EVO, 21.3R1-EVO, and all subsequent releases.

Note: Juniper SIRT's policy is not to evaluate releases which are beyond End of Engineering (EOE) or End of Life (EOL).

This issue is being tracked as 1604157.

Workaround

There are no viable workarounds for this issue.

To reduce the risk of exploitation use access lists or firewall filters to the device only from trusted, admini networks or hosts.

Modification History

2022-07-13: 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

AFFECTED PRODUCT SERIES / FEATURES