Cisco SD-WAN Solution Buffer Overflow Vulnerability (CVE-2020-3264)

High lbrossault published GHSA-wwq2-pxrj-v62r on Nov 20, 2021

Package

Viptela (Cisco)

Affected versions	Patched versions
18.3.8	18.4.5

Description

Overview

"confd_cli" is a client connecting to "confd" server in order to open a prompt. This binary has S-UID bit set and is vulnerable to a stack buffer overflow.
It can lead to a local escalation privilege.

This is finding has been observed on several components of the SD-WAN Cisco (Viptela) Solution but this vulnerability might also impact other products.

Detail

"confd_cli" has S-UID bit set. The purpose of this S-UID bit seems to allow this binary to access a secret file (shared with confd server) in order to perform a handshake and authenticate the client.
"confd_cli" execution can be configured through several environment variables.

"SSH_CONNECTION" environment variable is split into several arguments. The second argument of this environement is copyed into the stack with "sprintf()" without any length check.

By providing a long enough string the sprintf function overwrites buffers on the stack.

On Viptela this bug as been found on both controllers (vSmart, vManage and vBond) and boxes (vEdges) this binary is compiled without NX bit allowing to rewrite return address and redirect execution.

As the vulnerability is due to the use of sprintf(), null bytes are forbidden.

- vEdges are MIPS64 architectures compiled with big endian. That means that userland addresses are all stored starting with zeros. Therefore it is not possible to overwritte a valid address.
- Controllers are Intel x86_64 architectures. It is possible to redirect return address to a valid gadget.

In that second option a possible attack would be to pivot stack to a ROP chain (in a user handled memory area). That might result in a local privilege escalation.

Proof of Concept

By running following command:

```
vBondOLS:~$ SSH_CONNECTION="127.0.0.1
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
12" confd_cli
Segmentation fault (core dumped)
```

We can see that instruction pointer register is fully controlled allowing us to redirect execution to bad code:

```
vBondOLS:~$ dmesg |tail -n1
confd_cli[32379]: segfault at 6463626136 ip 0000006463626136 sp 00007fffd7a3b720 error 14 in libnsl-2.19.so[7f519f910000+14000]
```

Solution

Security patch

Cisco fixed this vulnerability from:

- sdwan-20.3.1 and later
- sdwan-20.3(0.43) and later
- sdwan-20.1.1 and later
- sdwan-20.1(0.301) and later
- sdwan-19.2.2 and later
- sdwan-18.4.5 and later

Workaround

There are no workarounds that address this vulnerability.

References

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwanbo-QKcABnS2
https://nvd.nist.gov/vuln/detail/CVE-2020-3264

Credits

Orange CERT-CC
Cyrille CHATRAS at Orange group

Timeline

Date reported: December 16, 2019
Date fixed: March 18, 2020

Severity

High 7.1 / 10

CVSS base metrics

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

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

CVE ID

CVE-2020-3264

Weaknesses

CWE-120