Security Advisory 2021-018

Critical Vulnerabilities in Cisco SD WAN vManage Software

April 8, 2021 — v1.0

TLP:WHITE

History:

- *8/04/2021 — v1.0 – Initial publication*

Summary

Cisco has published an advisory about several vulnerabilities affecting Cisco SD-WAN software [1-4]. These vulnerabilities could allow an unauthenticated, remote attacker to **execute arbitrary code** or allow an authenticated, local attacker to **gain escalated privileges** on an affected system. While Cisco is not aware of any malicious exploit in the wild, it is highly recommended to patch the affected products.

Technical Details

This advisory only describes the most critical vulnerabilities disclosed by Cisco for enterprise products.

CVE-2021-1479

The first vulnerability is due to improper validation of user-supplied input to the vulnerable component. An attacker could exploit this vulnerability by sending a crafted connection request to the vulnerable component that, when processed, could cause a buffer overflow condition. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system with *root* privileges.

CVE-2021-1137

The second vulnerability, is due to insufficient input validation by the affected software. An authenticated attacker who has permissions to add new users or groups on the vManage system could exploit this vulnerability by modifying a user account. A successful exploit could allow the attacker to gain *root* privileges on the underlying operating system.

CVE-2021-1480

The third vulnerability, is due to improper validation of input to the system file transfer functions. An authenticated attacker could exploit this vulnerability by sending specially crafted requests to the vulnerable system. A successful exploit could allow the attacker to overwrite

arbitrary files and modify the system in such a way that could allow the attacker to gain *root* privileges on the underlying operating system.

Affected Products

The following products could be affected by the vulnerabilities:

- IOS XE SD-WAN Software
- SD-WAN cEdge Routers
- SD-WAN vBond Orchestrator Software
- SD-WAN vEdge Routers
- SD-WAN vSmart Controller Software

The following software releases are affected by the vulnerabilities:

Cisco SD-WAN vManage Release	First Fixed Release
18.4 and earlier	Migrate to a fixed branch (19.2)
19.2	19.2.4
19.3	Migrate to a fixed branch (20.3 or later)
20.1	Migrate to a fixed branch (20.3 or later)
20.3	20.3.3
20.4	20.4.1

Recommendations

It is recommended to apply the patches from Cisco for all affected software and products.

References

[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-YuTVWqy

[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-1137

[3] https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-1479

[4] https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-1480