Security Advisory 2023-049

Critical Vulnerability in Cisco SD-WAN vManage

July 17, 2023 — v1.0

TLP:CLEAR

History:

- *17/07/2023 — v1.0 – Initial publication*

Summary

On July 12, 2023, Cisco released an advisory to address a critical vulnerability in the request authentication validation for the REST API of Cisco SD-WAN vManage software. Cisco SD-WAN vManage API is a REST API for controlling, configuring, and monitoring the Cisco devices in an overlay network. The vulnerability could allow an unauthenticated, remote attacker to gain read permissions or limited write permissions to the configuration of an affected Cisco SD-WAN vManage instance. It is tracked as `CVE-2023-20214` and has a CVSS score of 9.1.

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability [1].

Technical Details

This vulnerability is due to insufficient request validation when using the REST API feature. An attacker could exploit this vulnerability by sending a crafted API request to an affected vManage instance. A successful exploit could allow the attacker to retrieve information from and send information to the configuration of the affected Cisco vManage instance. This vulnerability only affects the REST API and does not affect the web-based management interface or the CLI [1].

Detection

Constituents may be able to detect attempts to access the REST API by examining the log file. The REST API log file is located at the following path in the vManage filesystem: `/var/log/nms/vmanage-server.log`. If the following line:

```
Request Stored in Map is (/dataservice/client/server) for user (admin)
```

appears in the log, the REST API has received requests [1].

Affected Products

Affected Cisco SD-WAN vManage Releases [1]:

- 20.6.3.3
- 20.6.4
- 20.6.5
- 20.7
- 20.8
- 20.9
- 20.10
- 20.11

Recommendations

CERT-EU strongly recommends update the affected versions of the software.

Workarounds

There are no workarounds that address this vulnerability. However, to mitigate this vulnerability and significantly reduce the attack surface, network administrators should enable access control lists (ACLs) to limit access to the vManage instance [1].

References

[1] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-unauthapi-sphCLYPA