Overall rating: Critical

BRITISH COLUMBIA

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware of a vulnerability in the request authentication validation for the REST API of Cisco SD-WAN vManage software that 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.

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.

This vulnerability is rated as a **Critical** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- Ensure mitigation is performed as soon as possible.

Please notify VRM with any questions or concerns you may have.

References

- Cisco Security Advisory - cisco-sa-vmanage-unauthapi-sphCLYPA
- Cisco Security Advisories