March 13, 2024

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that Cisco published security advisories to address vulnerabilities in multiple products. Included were updates for the following:

- Cisco IOS XR – multiple versions and platforms

Technical Details

A vulnerability in the request authentication validation for the REST API of Cisco SD-WAN vManage software 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. 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.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address these risks.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

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

References

- CVE-2024-28815 CVE-2024-20320 CVE-2024-20318 CVE-2024-20327 CVE-2023-20214 CVE-2024-20337 CVE-2024-20319 CVE-2024-20262 CVE-2024-20266 CVE-2024-20322 CVE-2024-20315
- Cisco Advisory – cisco-sa-iosxr-ssh-privesc-eWDMKew3
- Cisco Security Advisories