June 12, 2024

Overall Rating: Medium

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a vulnerability in the web-based management API of Cisco AsyncOS Software for Cisco Secure Email Gateway. The vulnerability affects Cisco AsyncOS Software versions 14.3 and earlier, 15.0 and 15.5.

Technical Details

A vulnerability in the web-based management API of Cisco AsyncOS Software for Cisco Secure Email Gateway could allow an unauthenticated, remote attacker to conduct an HTTP response splitting attack.

This vulnerability is due to insufficient input validation of some parameters that are passed to the web-based management API of the affected system. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to perform cross-site scripting (XSS) attacks, resulting in the execution of arbitrary script code in the browser of the targeted user, or could allow the attacker to access sensitive, browser-based information.

This vulnerability is rated as a **MEDIUM** risk. A software update exists to address this risk.

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 atVulnerabilityandRiskManagement@gov.bc.ca.

References

- CVE-2024-20392
- Cisco Secure Email Gateway HTTP Response Splitting Vulnerability
- VRM Vulnerability Reports