August 15, 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 scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance. The vulnerability affects Cisco Secure Web Appliance, both virtual and hardware versions, when the deflate, lzma, or brotli content-encoding type was enabled.

Technical Details

A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass a configured rule, allowing traffic onto a network that should have been blocked.

This vulnerability is due to improper detection of malicious traffic when the traffic is encoded with a specific content format. An attacker could exploit this vulnerability by using an affected device to connect to a malicious server and receiving crafted HTTP responses. A successful exploit could allow the attacker to bypass an explicit block rule and receive traffic that should have been rejected by the device.

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

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 at VulnerabilityandRiskManagement@gov.bc.ca.

References

- CVE-2023-20215
- Cisco Secure Web Appliance Content Encoding Filter Bypass Vulnerability
- VRM Vulnerability Reports