June 12, 2024

Overall Rating: Medium

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of multiple vulnerabilities in the web-based management interface of Cisco AsyncOS Software for Cisco Secure Email and Web Manager.

CVE-2024-20256 vulnerability affects versions of Secure Email and Web Manager, both virtual and hardware appliances and Secure Web Appliance, both virtual and hardware appliances.

CVE-2024-20257 affects Cisco Secure Email Gateway, both virtual and hardware appliances.

CVE-2024-20258 affects Cisco Secure Email and Web Manager, both virtual and hardware appliances and Secure Email Gateway, both virtual and hardware appliances

Technical Details

Multiple vulnerabilities in the web-based management interface of Cisco AsyncOS Software for Cisco Secure Email and Web Manager; Secure Email Gateway, formerly Email Security Appliance (ESA); and Secure Web Appliance could allow a remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface.

The vulnerabilities are not dependent on one another. Exploitation of one of the vulnerabilities is not required to exploit another vulnerability. In addition, a software release that is affected by one of the vulnerabilities may not be affected by the other vulnerabilities.

A vulnerability (CVE-2024-20258) in the web-based management interface of Cisco AsyncOS Software for Cisco Secure Email and Web Manager and Secure Email Gateway could allow an unauthenticated, remote attacker to conduct an XSS attack against a user of the interface.

This vulnerability is due to insufficient validation of user input. 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 execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.

A vulnerability (CVE-2024-20256) in the web-based management interface of Cisco AsyncOS Software for Cisco Secure Email and Web Manager and Secure Web Appliance could allow an authenticated, remote attacker to conduct an XSS attack against a user of the interface.

This vulnerability is due to insufficient validation of user input. 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 execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.

A vulnerability (CVE-2024-20257) in the web-based management interface of Cisco AsyncOS Software for Cisco Secure Email Gateway could allow an authenticated, remote attacker to conduct an XSS attack against a user of the interface.

This vulnerability is due to insufficient validation of user input. 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 execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.

A vulnerability (CVE-2024-20383) in the web-based management interface of Cisco AsyncOS Software for Cisco Secure Email and Web Manager could allow an authenticated, remote attacker to conduct an XSS attack against a user of the interface.

This vulnerability is due to insufficient validation of user input. 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 execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.

Cisco has released software updates that address these vulnerabilities. There are no workarounds that address these vulnerabilities.

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-2024-20256, CVE-2024-20257, CVE-2024-20258, CVE-2024-20383
- Cisco Secure Email and Web Manager, Secure Email Gateway, and Secure Web Appliance Cross-Site Scripting Vulnerabilities
- VRM Vulnerability Reports