March 6, 2024

Overall Rating - High

BRITISH COLUMBIA

This notification is intended as an informational bulletin 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 Secure Client – versions 4.10.04065 to versions prior to 4.10.08025
- Cisco Secure Client – version 5.0
- Cisco Secure Client – versions 5.1 prior to 5.1.2.42

Technical Details

A vulnerability in the SAML authentication process of Cisco Secure Client could allow an unauthenticated, remote attacker to conduct a carriage return line feed (CRLF) injection attack against a user.

This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a crafted link while establishing a VPN session. A successful exploit could allow the attacker to execute arbitrary script code in the browser or access sensitive, browser-based information, including a valid SAML token. The attacker could then use the token to establish a remote access VPN session with the privileges of the affected user. Individual hosts and services behind the VPN headend would still need additional credentials for successful access.

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

These vulnerabilities are rated as an overall **High** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

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

References

- CVE-2024-20337 CVE-2024-20338 CVE-2024-20335 CVE-2024-20336 CVE-2024-20292 CVE-2024-20346 CVE-2024-20345 CVE-2023-38545
- Cisco Advisory – cisco-sa-secure-client-crlf-W43V4G7
- Cisco Security Advisories