February 7, 2024

Overall rating: Critical

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 the following products:

- Cisco Expressway Series – versions prior to 14.3.4
- Secure Endpoint Connector for Windows – versions prior to 7.5.17 and 8.2.1
- Secure Endpoint Private Cloud – versions prior to 3.8.0

Technical Details

Two vulnerabilities in the API of Cisco Expressway Series devices could allow an unauthenticated, remote attacker to conduct CSRF attacks on an affected system.
These vulnerabilities are due to insufficient CSRF protections for the web-based management interface of an affected system. An attacker could exploit these vulnerabilities by persuading a user of the API to follow a crafted link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the affected user. If the affected user has administrative privileges, these actions could include modifying the system configuration and creating new privileged accounts.

These vulnerabilities are rated as an overall **Critical** 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-2024-20254 CVE-2024-20255
- Cisco Advisory - cisco-sa-expressway-csrf-KnnZDMj3
- Cisco Advisory - cisco-sa-clamav-hDffu6t
- Cisco Security Advisories