July 7, 2023

Overall rating: High

BRITISH COLUMBIA

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 Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches. The vulnerability affects Cisco Nexus 9000 Series Fabric Switches in ACI mode that are running releases 14.0 and later if they are part of a multi-Site topology and have the CloudSec encryption feature enabled.

Technical Details

A vulnerability in the Cisco ACI Multi-Site CloudSec encryption feature of Cisco Nexus 9000 Series Fabric Switches in ACI mode could allow an unauthenticated, remote attacker to read or modify inter-site encrypted traffic.

This vulnerability is due to an issue with the implementation of the ciphers that are used by the CloudSec encryption feature on affected switches. An attacker with an on-path position between the ACI sites could exploit this vulnerability by intercepting inter-site encrypted traffic and using cryptanalytic techniques to break the encryption. A successful exploit could allow the attacker to read or modify the traffic that is transmitted between the sites.

Cisco's Product Security Incident Response Team (PSIRT) is yet to find evidence of public exploit code targeting the vulnerability or that the flaw has been exploited in attacks.

Cisco has not released software updates to address the vulnerability that is described in this advisory. Customers who are currently using the Cisco ACI Multi-Site CloudSec encryption feature for the Cisco Nexus 9332C and Nexus 9364C Switches and the Cisco Nexus N9K-X9736C-FX Line Card are advised to disable it and to contact their support organization to evaluate alternative options.

This vulnerability is rated as a **HIGH** risk. A software patch 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.

References

- CVE-2023-20185
- Cisco ACI Multi-Site CloudSec Encryption Information Disclosure Vulnerability
- Cisco warns of bug that lets attackers break traffic encryption