September 14, 2023

Overall rating: Critical

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 remote access VPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software. The vulnerability Cisco devices if they were running a vulnerable release of Cisco ASA or FTD Software.

Technical Details

The impact of this vulnerability may allow an unauthenticated, remote attacker to conduct a brute force attack in an attempt to identify valid username and password combinations or an authenticated, remote attacker to establish a clientless SSL VPN session with an unauthorized user.

This vulnerability is due to improper separation of authentication, authorization, and accounting (AAA) between the remote access VPN feature and the HTTPS management and site-to-site VPN features. An attacker could exploit this vulnerability by specifying a default connection profile/tunnel group while conducting a brute force attack or while establishing a clientless SSL VPN session using valid credentials. A successful exploit could allow the attacker to achieve one or both of the following:

- Identify valid credentials that could then be used to establish an unauthorized remote access VPN session.
- Establish a clientless SSL VPN session (only when running Cisco ASA Software Release 9.16 or earlier).

Please note this vulnerability is reported as being exploited in the wild.

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

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address this risk.

Action Required

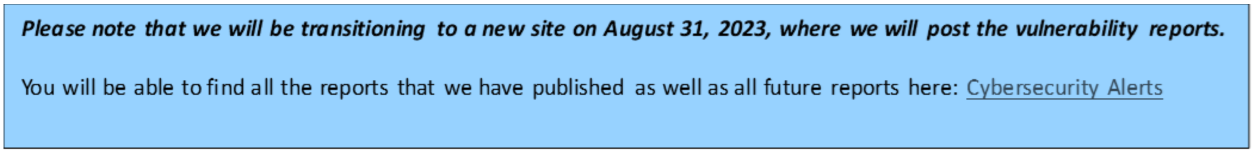
- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

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

References

- CVE-2023-20269
- Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Remote Access VPN Unauthorized Access Vulnerability
- Cisco warns of VPN zero-day exploited by ransomware gangs

Please note that we will be transitioning to a new site on August 31, 2023, where we will post the vulnerability reports.



Please note that we will be transitioning to a new site on August 31, 2023, where we will post the vulnerability reports.

You will be able to find all the reports that we have published as well as all future reports here: Cybersecurity Alerts

If you have any questions, please reach out to OCIOSecurity@gov.bc.ca