Security Advisory 2023-062

Cisco Remote Access VPN Vulnerability

September 11, 2023 — v1.0

TLP:CLEAR

History:

- *11/09/2023 — v1.0 – Initial publication*

Summary

On July 12, 2023, Cisco released an advisory to address a vulnerability in the remote access VPN feature of Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defence (FTD) software. It could 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 client-less SSL VPN session with an unauthorised user [1].

In addition, Cisco warns that the vulnerability could be actively exploited by ransomware groups to gain initial access to corporate networks [2].

Technical Details

This vulnerability is due to improper separation of authentication, authorisation, 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 client-less SSL VPN session using valid credentials. A successful exploit could allow the attacker to achieve one or both of the following [1]:

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

It is worth to note that:

- Establishing a client-based remote access VPN tunnel is not possible as these default connection profiles/tunnel groups do not and cannot have an IP address pool configured.
- This vulnerability does not allow an attacker to bypass authentication. To successfully establish a remote access VPN session, valid credentials are required, including a valid second factor if multi-factor authentication (MFA) is configured [1].

Detection

Indicators of compromise for this vulnerability are as follows [1]:

- Brute force attack: seeing a high rate of `syslog` message `%ASA-6-113015`, which reports a failed authentication attempt, can indicate a brute force or password spraying attack.
- Unauthorised client-less SSL VPN session establishment: Seeing a session establishment attempt (`syslog` message `%ASA-7-734003`) or termination event (`syslog` message `%ASA-4-113019`) that reports one of the following unexpected connection profiles/tunnel groups can indicate successful or attempted establishment of an unauthorised client-less SSL VPN session: `DefaultADMINGroup` or `DefaultL2LGroup`.

Affected Products

This vulnerability affected Cisco devices if they were running a vulnerable release of Cisco Adaptive Security Appliance (ASA) Software or Cisco Firepower Threat Defence (FTD) software and some conditions are met. Please refer to the Cisco advisory to find the conditions [1].

In addition, Cisco has confirmed that this vulnerability does not affect the following Cisco products [1]:

- Firepower Management Center (FMC) Software;
- FXOS Software;
- IOS Software;
- IOS XE Software;
- IOS XR Software;
- NX-OS Software.

Recommendations

Cisco will release software updates that address this vulnerability. Until fixes are made available, please review and implement workarounds that address this vulnerability.

Workarounds

While there is no method to completely prevent a brute force attack attempt, you can implement the following recommendations to protect against unauthorised client-less SSL VPN session establishment using the `DefaultADMINGroup` or `DefaultL2LGroup` connection profiles/tunnel groups [1]:

- configure a dynamic access policy (DAP) to terminate VPN tunnel establishment when the `DefaultADMINGroup` or `DefaultL2LGroup` connection profile/tunnel group is used;
- deny remote access VPN using the default group policy (`DfltGrpPolicy`);
- restrict users in the `LOCAL` user database
- lock users to a specific connection profile/tunnel group only;
- prevent users from establishing remote access VPN sessions.

References

[1] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ravpn-auth-8LyfCkeC#fs

[2] https://blogs.cisco.com/security/akira-ransomware-targeting-vpns-without-multi-factor-authentication