December 22, 2023

Overall rating: Medium

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 AnyConnect SSL VPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software. The vulnerability Cisco ASA Software and FTD Software if it had the AnyConnect SSL VPN feature enabled. The AnyConnect clientless SSL VPN feature is not affected.

Technical Details

A vulnerability in the AnyConnect SSL VPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to send packets with another VPN user's source IP address.

This vulnerability is due to improper validation of the packet's inner source IP address after decryption. An attacker could exploit this vulnerability by sending crafted packets through the tunnel. A successful exploit could allow the attacker to send a packet impersonating another VPN user's IP address. It is not possible for the attacker to receive return packets.

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

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

This vulnerability is rated as a **MEDIUM** 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-2023-20275
- Cisco Adaptive Security Appliance and Firepower Threat Defense Software VPN Packet Validation Vulnerability
- VRM Vulnerability Reports