December 1, 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 Cisco Secure Client Software, formerly AnyConnect Secure Mobility Client vulnerability. The vulnerability affects at the time of publication, if they were running a vulnerable release of software: Secure Client AnyConnect for Android, Secure Client AnyConnect VPN for iOS, Secure Client (including AnyConnect) for Universal Windows Platform, Secure Client for Linux and Secure Client for MacOS.

Technical Details

Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure Mobility Client, may allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected system.

These vulnerabilities are due to an out-of-bounds memory read from Cisco Secure Client Software. An attacker could exploit these vulnerabilities by logging in to an affected device while another user is accessing Cisco Secure Client on the same system, and then sending crafted packets to a port on that local host. A successful exploit could allow the attacker to crash the VPN Agent service, causing it to be unavailable to all users of the system. To exploit these vulnerabilities, the attacker must have valid credentials on a multi-user system.

Exploitability Metrics
Attack Vector: Local
Attack Complexity: Low
Privileges Required: Low
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-2023-20240, CVE-2023-20241
- Cisco Secure Client Software Denial of Service Vulnerabilities
- VRM Vulnerability Reports