Overall Rating - High

BRITISH COLUMBIA

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that on August 8, 2023, the paper Bypassing Tunnels: Leaking VPN Client Traffic by Abusing Routing Tables was made public.

Vulnerable Products

These attacks affect Cisco Secure Client AnyConnect VPN for iOS regardless of client configuration and the following products if they are deployed with an affected configuration:

- Cisco AnyConnect Secure Mobility Client for Linux
- Cisco AnyConnect Secure Mobility Client for MacOS
- Cisco AnyConnect Secure Mobility Client for Windows
- Cisco Secure Client for Linux
- Cisco Secure Client for MacOS
- Cisco Secure Client for Windows

Technical Details

The paper discusses two attacks that can cause VPN clients to leak traffic outside the protected VPN tunnel. In both instances, an attacker can manipulate routing exceptions that are maintained by the client to redirect traffic to a device that they control without the benefit of the VPN tunnel encryption.

- CVE-2023-36672 - For the LocalNet attacks to be successful, a client must be configured to allow local LAN access. The default policy for clients is to deny local LAN access. As a result, clients in a default configurations are not affected by the LocalNet attacks.

- CVE-2023-36673 - For the ServerIP attacks, customers who use the Umbrella Roaming Security module is protected against DNS spoofing attacks

These vulnerabilities are rated as an overall **High** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

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

References

- CVE-2023-36672, CVE-2023-36673

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ac-leak-Sew6g2kd