مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerability in AWS ClientVPN macOS Client

Tracking #:432317790

Date:08-10-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed AWS has released a fix for critical local privilege escalation in the macOS AWS Client VPN Client.

TECHNICAL DETAILS:

AWS has released a fix for CVE-2025-11462, a local privilege escalation in the macOS AWS Client VPN Client. A non-admin user could create a symlink from a client log file to a privileged location and cause arbitrary content to be written there during log rotation, permitting root-level code execution.

Vulnerability Details:

1. **CVE-2025-11462**: API Key Disclosure & User Enumeration
   - **CVSS 4.0: 9.3(Critical)**
   - Affected software: AWS Client VPN macOS client, versions 1.3.2 through 5.2.0. Not affecting Windows or Linux clients.
   - Root cause: insufficient validation of the log destination during log rotation; attacker-controlled symlink could redirect log writes to privileged files (e.g., crontab), allowing arbitrary content to be written with elevated privileges and executed.
   - Fixed Version: AWS Client VPN Client version 5.2.1

RECOMMENDATIONS:

- Apply Patches Immediately: Upgrade all macOS endpoints running the AWS Client VPN Client to fixed version or later.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://aws.amazon.com/security/security-bulletins/AWS-2025-020/