مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in AWS Client VPN for Windows

Tracking #:432317525

Date:24-07-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in AWS Client VPN for Windows that could be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

Amazon Web Services (AWS) has released a security update addressing a high-severity local privilege escalation vulnerability (CVE-2025-8069) in the AWS Client VPN software for Windows. The flaw could allow non-administrative users to gain SYSTEM-level privileges during installation, posing significant risk in enterprise environments and shared systems.

Vulnerability Details:

- CVE-2025-8069
- CVSS Score 7.3 High
- The vulnerability arises from the way the installer references an OpenSSL configuration file during the setup process. Specifically, the installer accesses the following hardcoded path:
  - C:\usr\local\windows-x86_64-openssl-localbuild\ssl
- This directory is writable by low-privileged users. If a malicious user creates a crafted OpenSSL configuration file at this location, and an administrator subsequently installs the VPN client, the configuration can be used to execute arbitrary code with elevated privileges.

Impact:

Successful exploitation may allow a local attacker with limited access to escalate privileges to SYSTEM—effectively taking full control of the system. This risk is especially high on multi-user or managed devices.

Affected Versions:

- AWS Client VPN for Windows 4.1.0, 5.0.0, 5.0.1, 5.0.2, 5.1.0, 5.2.0, 5.2.1

Fixed Version

- AWS Client VPN for Windows 5.2.2 or later.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Amazon Web Services (AWS).

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-2025-014/