مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Script Injection Vulnerability in OpenVPN
Tracking #:432317866
Date:28-10-2025

TLP: WHITE

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability has been identified in the development preview versions of OpenVPN.

TECHNICAL DETAILS:

A high-severity vulnerability has been identified in the development preview versions of OpenVPN (2.7_alpha1 through 2.7_beta1). This flaw, tracked as CVE-2025-10680, is a script injection vulnerability that could allow a malicious or compromised VPN server to execute arbitrary commands on a connecting client's system.

The vulnerability stems from improper sanitization of pushed DNS and DHCP options. When these options are passed to the client's --dns-updown script hook, specially crafted arguments can inject and execute additional shell commands. Successful exploitation could lead to a full compromise of the client device, especially if the OpenVPN client process runs with elevated privileges.

The OpenVPN team has addressed this issue in the 2.7_beta2 release. OpenVPN 2.6.x and earlier stable releases are not affected.

Vulnerability Details
- CVE ID: CVE-2025-10680
- Severity: High (CVSS 8.8)
- Affected Versions: OpenVPN 2.7_alpha1 → 2.7_beta1
- Fixed Version: OpenVPN 2.7_beta2
- Affected Platforms:
  - Unix-like systems (Linux, BSD, macOS)
  - Windows systems only if configured to use the same DNS-updown PowerShell call

RECOMMENDATIONS:

- Upgrade Immediately: All users, administrators, and developers using affected versions of OpenVPN must upgrade to fixed or a later version without delay.

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://www.mail-archive.com/openvpn-announce@lists.sourceforge.net/msg00149.html