CVE-2025-50054: Buffer Overflow In OpenVPN

Vairav CVE Report

Date: June 23, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

A single vulnerability, **CVE-2025-50054**, has been identified in the OpenVPN ovpn-dco-win Windows kernel driver. The vulnerability is a heap-based buffer overflow that can be exploited locally to cause a denial-of-service (DoS) condition by crashing the system. Although a CVSS score has not been assigned yet, this vulnerability is severe. Though it cannot be exploited remotely or for privilege escalation, it still poses a significant risk due to its ability to destabilize affected systems and organizations using affected versions should upgrade promptly.

VULNERABILITY DETAILS

CVE-2025-50054

- **Description:** A heap-based buffer overflow exists in the ovpn-dco-win kernel driver component of OpenVPN. The flaw can be triggered by sending a control packet larger than 1500 bytes to the driver, exceeding its expected buffer size and causing a crash. This can be done by any local process, including those without administrative privileges. The official OpenVPN client enforces correct message size and does not trigger the vulnerability; however, custom clients or tools can exploit this condition.
- **Impact:** Exploitation results in a system-wide denial-of-service (DoS) due to a kernel driver crash. No remote code execution or privilege escalation is possible, but system stability is compromised.
- **CVSS Score:** N/A

AFFECTED VERSIONS

- OpenVPN ovpn-dco-win driver versions <= 1.3.0 and versions <= 2.5.8.
- OpenVPN GUI for Windows version 2.6.0-I005 through 2.6.14-I001 and version 2.7_alpha1-I001 are affected.

EXPLOIT DETAILS

These vulnerabilities particularly concern environments where the **ovpn-dco-win** driver is used to accelerate OpenVPN connections on Windows systems. Exploitation could lead to denial-of-service by crashing the Windows kernel. A potential attack scenario includes:

- A local application (even with limited privileges) crafts a malformed control packet larger than 1500 bytes.
- The packet is sent to the OpenVPN driver.
- The driver overflows its internal buffer, causing a kernel panic and crashing the system.

RECOMMENDED ACTIONS

Patch & Upgrade

Upgrade to the latest OpenVPN GUI for Windows versions with patched ovpn:

- 2.6.14-I002
- 2.7_alpha2-I001

ADDITIONAL SECURITY MEASURES

- Limit local access to the ovpn-dco-win device driver through file system or ACL-based restrictions.
- Use Endpoint Detection & Response (EDR) tools to detect abnormal driver interaction or large malformed packet transmissions.
- Prevent installation of or access to unauthorized OpenVPN clients or third-party networking tools on managed endpoints.
- Monitor system logs for recurring crashes or driver-level errors associated with ovpn-dco-win.

REFERENCES

- https://app.opencve.io/cve/CVE-2025-50054
- https://cybersecuritynews.com/openvpn-driver-vulnerability/

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com