Security Advisory 2024-076

Vulnerabilities in OpenVPN

August 12, 2024 — v1.0

TLP:CLEAR

History:

- *12/08/2024 — v1.0 – Initial publication*

Summary

On March 20, 2024, the OpenVPN community project team disclosed several vulnerabilities, **CVE-2024-27459**, **CVE-2024-24974**, **CVE-2024-27903** and **CVE-2024-1305** that could be chained to achieve remote code execution (RCE) and local privilege escalation (LPE) [1].

On August 8, 2024, Microsoft released a writeup for those vulnerabilities [2].

Technical Details

- CVE-2024-27459: Vulnerability in the communication mechanism between the `openvpn.exe` process and the `openvpnserv.exe` service.
- CVE-2024-24974: Vulnerability involving unprivileged access to an operating system resource. The `openvpnserv.exe` service spawns a new `openvpn.exe` process based on user requests received through the `\\openvpn\\service` named pipe.
- CVE-2024-27903: Vulnerability in OpenVPN's plugin mechanism that permits plugins to be loaded from various paths on an endpoint device.
- CVE-2024-1305: Vulnerability in the "tap-windows6" project that involves developing the Terminal Access Point (TAP) adapter used by OpenVPN. In the project's src folder, the `device.c` file contains the code for the TAP device object and its initialisation.

You can find the complete technical explanation in the Microsoft report [2].

Affected Products

All versions of OpenVPN prior to version 2.6.10 (and 2.5.10).

Recommendations

CERT-EU recommends OpenVPN users to apply the latest security updates as soon as possible [3].

References

[1] https://forums-new.openvpn.net/forum/announcements/69-release-openvpn-version-2-6-10

[2] https://www.microsoft.com/en-us/security/blog/2024/08/08/chained-for-attack-openvpn-vulnerabilities-discovered-leading-to-rce-and-lpe/

[3] https://openvpn.net/community-downloads/