

HiveForce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## Chained Exploits: OpenVPN Vulnerabilities Lead to RCE and LPE

Date of Publication

August 13, 2024

Admiralty Code

A1

TA Number

TA2024309













# Summary

**First Seen:** July 2024

**Affected Products:** OpenVPN

**Impact:** Multiple vulnerabilities have been identified in OpenVPN, a widely used open-source VPN software. When exploited together in an attack chain, these vulnerabilities enable attackers to achieve both remote code execution (RCE) and local privilege escalation (LPE). This potential attack chain poses a significant security threat, as it could allow attackers to gain complete control over targeted endpoints, leading to data breaches, system compromises, and unauthorized access to sensitive information.

## CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-27459	OpenVPN Stack Overflow Vulnerability	OpenVPN			
CVE-2024-24974	OpenVPN Unauthorized Access Vulnerability	OpenVPN			
CVE-2024-27903	OpenVPN Remote Code Execution Vulnerability	OpenVPN			
CVE-2024-1305	OpenVPN Windows TAP Memory Overflow Vulnerability	Windows TAP driver			

## Vulnerability Details

### #1

Multiple medium-severity vulnerabilities have been identified in OpenVPN, a widely deployed open-source VPN software. Although these vulnerabilities alone may not be critical, they have the potential to be chained together, leading to system compromise, data breaches, unauthorized access, and other security issues. Exploiting these flaws requires user authentication, a deep understanding of OpenVPN's architecture, and intermediate knowledge of operating systems, making this a more challenging attack vector.

## #2

The flaws were identified within OpenVPN's client-side architecture, specifically in the interaction between the `openvpn.exe` process and the `openvpnserv.exe` service. CVE-2024-27459 and CVE-2024-24974 are flaws within the `openvpnserv.exe` service that could result in DoS and LPE on Windows systems. Meanwhile, CVE-2024-27903 is a vulnerability in the plugin mechanism that could lead to RCE on Windows, and LPE as well as data manipulation on Android, iOS, macOS, and BSD systems. Additionally, CVE-2024-1305 is a memory overflow vulnerability in the Windows TAP driver (`tap-windows6` project), potentially triggering a DoS attack.

## #3

Although these vulnerabilities are not easily exploitable on their own, they could be chained together by a skilled attacker to create a sophisticated attack chain, combining RCE and LPE. Typically, an attacker would need to gain access to a user's OpenVPN credentials through methods such as credential theft, info-stealing malware, or network traffic sniffing.

## #4

An attacker could exploit vulnerabilities like CVE-2024-24974 and CVE-2024-27903 to execute arbitrary code on a victim's device. This could be done by sending a specially crafted request to the OpenVPN service, which would launch a new instance with a malicious configuration file, allowing the attacker to access and manipulate sensitive data. Additionally, by exploiting CVE-2024-27459 and CVE-2024-27903, an attacker could achieve LPE by loading a malicious plugin into OpenVPN, thereby bypassing security restrictions and gaining administrative control over the device.

## #5

By chaining at least three of the four identified vulnerabilities, an attacker could achieve both RCE and LPE, creating a formidable attack vector. Techniques such as BYOVD could be employed following LPE to further compromise the system. Organizations using OpenVPN should promptly apply security updates and patches to mitigate these vulnerabilities.

## Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-27459	OpenVPN Version: Prior to 2.5.10	cpe:2.3:a:openvpn:openvpn:*:*:*:community:*:*	CWE-121
CVE-2024-24974	OpenVPN Version: Prior to 2.5.10	cpe:2.3:a:openvpn:openvpn:*:*:*:community:*:*	CWE-923
CVE-2024-27903	OpenVPN Version: Prior to 2.5.10	cpe:2.3:a:openvpn:openvpn:*:*:*:community:*:*	CWE-283
CVE-2024-1305	tap-windows6 driver Version: Prior to 9.26	cpe:2.3:a:openvpn:tap-windows:*:*:*:*:*	CWE-190

# Recommendations



**Apply Patch:** To mitigate the risks associated with these vulnerabilities, users are strongly advised to upgrade their OpenVPN installations to the latest versions (2.6.10 or 2.5.10). This upgrade addresses the identified vulnerabilities and helps protect against potential exploits.



**Vulnerability Management:** Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.



**Least Privilege:** Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks, restrict the access to the trusted parties only. This strategy reduces the effects of vulnerabilities related to privilege escalation.



**Implement Strong Authentication:** It is recommended to implement strong authentication measures and minimize the number of users with write access to critical systems. This approach will enhance security by reducing the risk of unauthorized access and potential exploitation of vulnerabilities.

## Potential MITRE ATT&CK TTPs

<b>TA0042</b> Resource Development	<b>TA0001</b> Initial Access	<b>TA0002</b> Execution	<b>TA0004</b> Privilege Escalation
<b>TA0040</b> Impact	<b>T1588</b> Obtain Capabilities	<b>T1588.006</b> Vulnerabilities	<b>T1190</b> Exploit Public-Facing Application
<b>T1059</b> Command and Scripting Interpreter	<b>T1498</b> Network Denial of Service	<b>T1068</b> Exploitation for Privilege Escalation	<b>T1203</b> Exploitation for Client Execution



## Patch Details

To mitigate these risks, users are strongly urged to immediately update their OpenVPN installations to the latest versions (2.6.10 or 2.5.10).

Link:

<https://www.mail-archive.com/openvpn-users@lists.sourceforge.net/msg07534.html>

## References

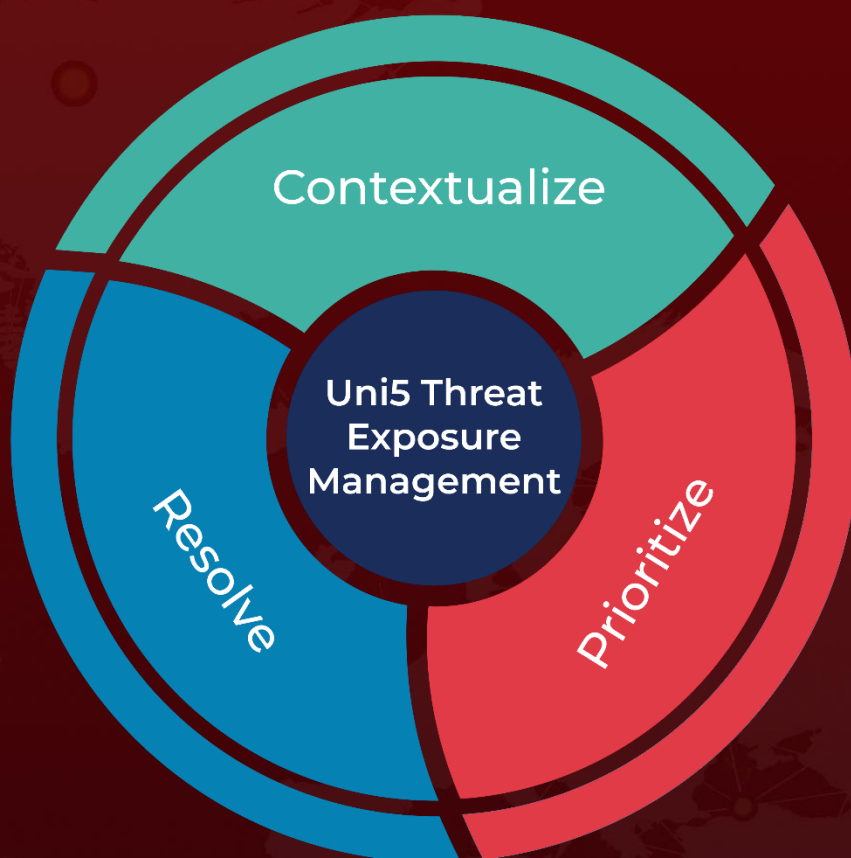
<https://openvpn.net/security-advisory/ovpnx-vulnerability-cve-2024-27903-cve-2024-27459-cve-2024-24974/>

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

# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

**August 13, 2024 • 4:15 AM**

© 2024 All Rights are Reserved by Hive Pro



More at [www.hivepro.com](http://www.hivepro.com)