مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

RCE and LPE Vulnerabilities in OpenVPN

Tracking #:432316136

Date:12-08-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in OpenVPN that could be exploited in a chained attack, leading to remote code execution (RCE) and local privilege escalation (LPE).

TECHNICAL DETAILS:

Microsoft disclosed four security flaws in the open-source OpenVPN software that could be chained to achieve remote code execution (RCE) and local privilege escalation (LPE). This attack chain could enable attackers to gain full control over targeted endpoints, potentially resulting in data breaches, system compromise, and unauthorized access to sensitive information.

Vulnerability Details:

- **CVE-2024-1305** | Base score: 9.8 – Critical
  - A memory overflow vulnerability leading to DoS in Windows
- **CVE-2024-27459** | Base score: 7.8 – High
  - A stack overflow vulnerability leading to a Denial-of-service (DoS) and LPE in Windows
- **CVE-2024-24974** | Base score: 7.5 – High
  - Unauthorized access to the "\\openvpn\\service" named pipe in Windows, allowing an attacker to remotely interact with it and launch operations on it
- **CVE-2024-27903** | Base score: 7.2 – High
  - A vulnerability in the plugin mechanism leading to RCE in Windows, and LPE and data manipulation in Android, iOS, macOS, and BSD

The first three of the four flaws are rooted in a component named openvpnserv, while the last one resides in the Windows Terminal Access Point (TAP) driver. An attacker could potentially exploit at least three of the four identified vulnerabilities to achieve Remote Code Execution (RCE) and Local Privilege Escalation (LPE). These exploits could be combined to form a formidable attack chain.

Attack Chain:

The attack chain involves several steps:

- **Credential Theft**: Attackers must first obtain the OpenVPN user's credentials, which can be achieved through various means, including malware or purchasing stolen credentials.
- **Exploitation**: Once credentials are obtained, attackers can use them to access the OpenVPN service and execute malicious commands, potentially leading to RCE and LPE.
- **Malicious Plugin Loading**: Attackers can exploit vulnerabilities to load harmful plugins, enabling further control over the system.

Fixed Versions:

- Versions 2.6.10 and 2.5.10

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to install the fixed version or latest version released by OpenVPN.

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