BLACKSWAN CYBERSECURITY

THREAT ADVISORY

August 14, 2024

OpenVPN Vulnerabilities lead to RCE and LPE

SUMMARY

Microsoft reported four medium-severity vulnerabilities in OpenVPN that could be combined to enable remote code execution (RCE) and local privilege escalation (LPE). "Exploiting this attack chain could allow attackers to take full control of targeted endpoints, potentially leading to data breaches, system compromises, and unauthorized access to sensitive information," stated Vladimir Tokarev from the Microsoft Threat Intelligence Community.

TECHNICAL DETAILS

Researchers discovered vulnerabilities while analyzing the OpenVPN open-source project to improve enterprise security standards. During this examination, they also reviewed two other popular VPN solutions and identified that they were vulnerable to a specific flaw (CVE-2024-1305), which led them to further investigate open-source VPN projects. Upon confirming that the same vulnerability existed in the OpenVPN repository, the research focused on evaluating the architecture and security model of OpenVPN, particularly for Windows systems.

List of Vulnerabilities:

- CVE-2024-27459: A stack overflow vulnerability in Windows leading to a Denial-of-Service (DoS) and Local Privilege Escalation (LPE).
- CVE-2024-24974: Unauthorized access to the "openvpnservice" named pipe in Windows, allowing remote attackers to interact with it and perform operations.
- CVE-2024-27903: A flaw in the plugin mechanism causing Remote Code Execution (RCE) in Windows, and LPE and data manipulation in Android, iOS, macOS, and BSD.
- CVE-2024-1305: A memory overflow vulnerability in the Windows Terminal Access Point (TAP) driver, leading to DoS.

The first three vulnerabilities are linked to a component named openvpnserv, while the fourth is related to the Windows TAP driver. These vulnerabilities can be exploited if an attacker gains access to a user's OpenVPN credentials. Such credentials can be acquired through methods like purchasing stolen data on the dark web, deploying stealer malware, or capturing network traffic to obtain NTLMv2 hashes and cracking them using tools like HashCat or John the Ripper.

Attackers can chain these vulnerabilities by combining, for example, CVE-2024-24974 with CVE-2024-27903 or CVE-2024-27459 with CVE-2024-27903—to achieve RCE and LPE. Vladimir Tokarev noted that at least three of the four discovered flaws could be leveraged to construct a potent attack chain, including techniques like Bring Your Own Vulnerable Driver (BYOVD). This could allow attackers to disable critical security processes, such as Microsoft Defender's Protect Process Light (PPL), bypass security products, and manipulate core system functions, making detection and mitigation more challenging.

Hunting Queries:

Detecting Remote Connections to OpenVPN's Named Pipe:

```
DeviceEvents
| where ActionType == "NamedPipeEvent"
| extend JsonAdditionalFields="parse_json(AdditionalFields)"
| extend PipeName="JsonAdditionalFields["PipeName"]"
| where PipeName == "\Device\NamedPipe\openvpn\service" and isnotempty(RemoteIP)
```

Identifying Image Load from Shared Folder into OpenVPN's Process:

```
DeviceImageLoadEvents
 | where InitiatingProcessFileName == "openvpn.exe" and FolderPath startswith "\\"
```

Detecting Unauthorized Process Connection to OpenVPN's Named Pipe:

```
DeviceEvents
| where ActionType == "NamedPipeEvent"
| extend JsonAdditionalFields="parse_json(AdditionalFields)"
| extend PipeName="JsonAdditionalFields["PipeName"],"
NamedPipeEnd="JsonAdditionalFields["NamedPipeEnd"]"
| where PipeName == "\Device\NamedPipe\openvpn\service" and NamedPipeEnd == "Server" and
InitiatingProcessFileName != "openvpnserv.exe"
```

RECOMMENDATIONS

Patch Vulnerable Versions:

- Ensure that OpenVPN versions prior to 2.5.10 and 2.6.10 are updated. Apply the necessary patches from the OpenVPN website.
- Security Best Practices:
- Disconnect OpenVPN clients from the internet and segment them within the network.
- Restrict access to OpenVPN clients to authorized users only.
- Prioritize patching while ensuring proper network segmentation, enforcing strong passwords, and minimizing the number of users with write authentication.

REFERENCES

- https://www.microsoft.com/en-us/security/blog/2024/08/08/chained-for-attack-openvpn-vulnerabilities-discovered-leading-to-rce-and-lpe/
- https://blackhat.com/us-24/briefings/schedule/#ovpnx-zero-days-leading-to-rce-lpe-and-kce-via-byovd-affecting-millions-of-openvpn-endpoints-across-the-globe-38900
- https://enlyft.com/tech/products/openvpn
- https://github.com/OpenVPN/openvpn/blob/v2.6.10/Changes.rst
- https://github.com/OpenVPN/openvpn/blob/v2.5.10/Changes.rst
- https://forums-new.openvpn.net/forum/announcements/69-release-openvpn-version-2-6-10
- https://openvpn.net/community-downloads/
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-27459 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-24974

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-27903 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-1305
- https://openvpn.net/as-docs/site-to-site-routing.html#site-to-site-routing
- https://openvpn.net/community-resources/reference-manual-for-openvpn-2-4/
- https://github.com/OpenVPN/openvpn/blob/master/include/openvpn-plugin.h.in
- https://www.lifewire.com/net-use-command-2618096
- https://wikipedia.org/wiki/Stack_buffer_overflow#Stack_canaries
- https://community.openvpn.net/openvpn/wiki/Downloads
- https://www.cisa.gov/secure-our-world/use-strong-passwords
- https://thehackernews.com/2024/08/microsoft-reveals-four-openvpn-flaws.html