VPN Clients Security Testing

Windows Client Validation Retest

NordVPN

Monday, March 15, 2021

VerSprite OffSec Team

Table of Contents

Validation Retest Matrix

Vulnerability	Status	Summary
Sensitive Information Found in Memory (CWE-316)	Remediated	During the validation retest, VerSprite discovered that it is no longer possible to extract the user credentials from the NordVPN client process memory. In the newly tested version, the authentication process occurs in the web browser instead.
Lack of Compile-Time Protections (CWE-693)	Mitigated	We found that some of the NordVPN client binaries were still missing some of the available compile time protections. However, the new binaries made use of more protections than the previous version, indicating good progress in this direction.
Outdated Version of OpenSSL (CWE-1104)	Remediated	The version of OpenSSL bundled with the newer version of NordVPN was 2.4.10. This is a much more recent version and there are no publicly known vulnerabilities or exploits for it.

Figure 1 – Validation Retest Matrix

(Remediated) Sensitive Information Found in Memory (CWE-316) – Low

Validation Retest Notes

During the validation retest, VerSprite discovered that it is no longer possible to extract the user credentials from the NordVPN client process memory. In the newly tested version, the authentication process occurs in the web browser instead.

As can be seen in the following command output, it was no longer possible to find the user's password in the process memory of either the GUI or the service:

```
C:\Python27\Scripts> ..\python.exe pfind.py -x 4d00560400620070004100410042003800730060042006a007800
nordvpn-service.exe NordVPN.exe

Process memory finder
[redacted]


C:\Python27\Scripts>
```

(Mitigated) Lack of Compile-Time Protections (CWE-693) – Low

Validation Retest Notes

During the validation retest, we found that some of the NordVPN client binaries were still missing some of the available compile time protections. However, the new binaries made use of more protections than the previous version, indicating good progress in this direction.

The following output of the *winchecksec* tool shows the improvements, as well as the protections that are still not in use:

```
./Program Files/NordVPN/6.35.2.0/Resources/Binaries/32bit/openvpn-nordvpn.exe
Dynamic Base    : "Present"
ASLR            : "Present"
High Entropy VA : "NotPresent"
Force Integrity : "Present"
Isolation       : "Present"
NX              : "Present"
SEH             : "Present"
CFG             : "Present"
RFG             : "Present"
SafeSEH         : "NotPresent"
GS              : "Present"
Authenticode    : "Present"
.NET            : "NotPresent"

./Program Files/NordVPN/6.35.2.0/Resources/Binaries/32bit/devcon.exe
Dynamic Base    : "Present"
ASLR            : "Present"
High Entropy VA : "NotPresent"
Force Integrity : "NotPresent"
Isolation       : "Present"
NX              : "Present"
SEH             : "Present"
CFG             : "Present"
RFG             : "Present"
SafeSEH         : "NotPresent"
GS              : "Present"
Authenticode    : "Present"
.NET            : "NotPresent"

./Program Files/NordVPN/6.35.2.0/Resources/Binaries/64bit/openvpn-nordvpn.exe
Dynamic Base    : "Present"
ASLR            : "Present"
High Entropy VA : "Present"
Force Integrity : "Present"
Isolation       : "Present"
NX              : "Present"
SEH             : "Present"
CFG             : "Present"
RFG             : "NotPresent"
SafeSEH         : "NotApplicable"
GS              : "Present"
Authenticode    : "Present"
.NET            : "NotPresent"

./Program Files/NordVPN/6.35.2.0/Resources/Binaries/64bit/devcon.exe
```

```
Dynamic Base    : "Present"
ASLR            : "Present"
High Entropy VA : "Present"
Force Integrity : "NotPresent"
Isolation       : "Present"
NX              : "Present"
SEH             : "Present"
CFG             : "Present"
RFG             : "NotPresent"
SafeSEH         : "NotApplicable"
GS              : "Present"
Authenticode    : "Present"
.NET            : "NotPresent"
```

(Remediated) Outdated Version of OpenSSL (CWE-1104) – Low

Validation Retest Notes

The version of OpenSSL bundled with the newer version of NordVPN was 2.4.10, released 9 December, 2020. The latest version at the time of writing is 2.5.1, released 24 February, 2021. This is a much more recent version and there are no publicly known vulnerabilities or exploits for it.

```
C:\Program Files\NordVPN\6.35.2.0\Resources\Binaries\64bit>openvpn-nordvpn.exe --version
OpenVPN 2.4.10 Windows-MSVC [SSL (OpenSSL)] [LZO] [LZ4] [PKCS11] built on Feb 15 2021
library versions: OpenSSL 1.1.1i  8 Dec 2020, LZO 2.10
Windows version 6.2 (Windows 8 or greater) 64bit
Originally developed by James Yonan
Copyright (C) 2002-2018 OpenVPN Inc <sales@openvpn.net>
Compile time defines: N/A

C:\Program Files\NordVPN\6.35.2.0\Resources\Binaries\64bit>
```

The CVE details page from MITRE shows no publicly known vulnerabilities and exploits for this version: https://www.cvedetails.com/vulnerability-list/vendor_id-3278/product_id-5768/Openvpn-Openvpn.html

The OpenVPN changelog at https://openvpn.net/community-downloads/ also shows no security patches being applied.