nmht3t Follow

Sep 16, 2020 · 2 min read · Listen

[CVE-2020–25744] SaferVPN for Windows Arbitrary File Overwrite DoS

Description

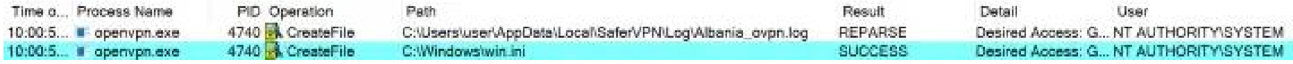
SaferVPN for Windows can be forced to overwrite an arbitrary file. SaferVPN for Windows spawns **openvpn.exe** which runs with SYSTEM privileges, and the **openvpn.exe** process creates a log file named `xxx_ovpn.log` under `%USERPROFILE%\AppData\Local\SaferVPN\Log` (xxx is the name of the country you are connecting to, for example, `Albania_ovpn.log`). Since the user has full control over the log folder, it is possible to delete all files under the log folder and create a symbolic link pointing to a high privileged file such as `C:\Windows\win.ini`. As a result, the contents of the log file created by the **openvpn.exe** will be overwritten on the high privileged file. Due to the lack of control over the file's content, the only potential attack vector is denial of service.

Exploitation

1. Delete files under `%USERPROFILE%\AppData\Local\SaferVPN\Log\` folder.
2. Use the CreateSymlink.exe tool from googleprojectzero's symboliclink-testing-tools to create a symbolic link on `%USERPROFILE%\AppData\Local\SaferVPN\Log\Albania_ovpn.log` that points to `C:\Windows\win.ini`. (it should be noted that the name of the log file must be changed according to which country you are connecting to, let's say if you connect to Austria, it should be named as `Austria_ovpn.log`)
3. Click the `Connect` button in SaferVPN for Windows app.
4. The `C:\Windows\win.ini` file will be overwritten with the contents of the log file.

Proof of Concept

The below screenshot shows that the **openvpn.exe** process reparsing the symbolic link we created when accessing the `Albania_ovpn.log` file and overwriting the `C:\Windows\win.ini` file.



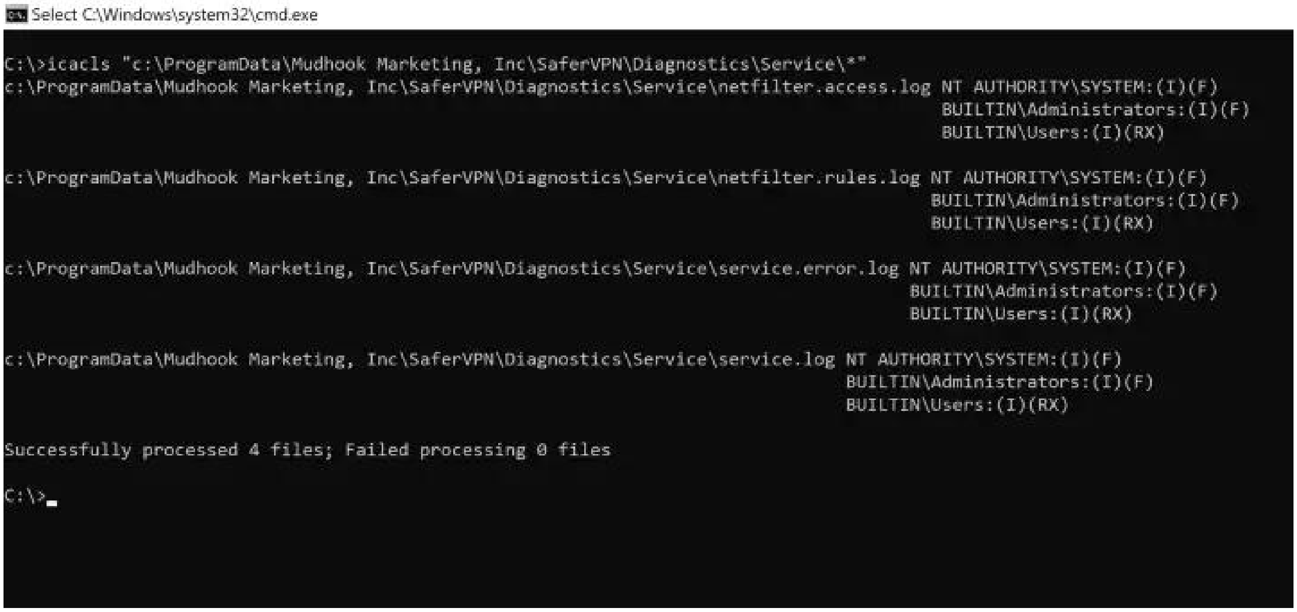
Time o...	Process Name	PID	Operation	Path	Result	Detail	User
10:00:5...	openvpn.exe	4740	CreateFile	C:\Users\user\AppData\Local\SaferVPN\Log\Albania_ovpn.log	REPARSE	Desired Access: G...	NT AUTHORITY\SYSTEM
10:00:5...	openvpn.exe	4740	CreateFile	C:\Windows\win.ini	SUCCESS	Desired Access: G...	NT AUTHORITY\SYSTEM

Step by step PoC video

SaferVPN for Windows Arbitrary File Overwrite DoS (CVE-2020–2…

Fix

The vendor silently fixed this vulnerability in version 5.0.3.3 by not creating the `Albania_ovpn.log` file and the entire log folder is moved to `C:\ProgramData\Mudhook Marketing, Inc\SaferVPN\Diagnostics\Service` with proper permissions set.



```
C:\>icacls "c:\ProgramData\Mudhook Marketing, Inc\SaferVPN\Diagnostics\Service\*"
c:\ProgramData\Mudhook Marketing, Inc\SaferVPN\Diagnostics\Service\netfilter.access.log NT AUTHORITY\SYSTEM:(I)(F)
                                                                                        BUILTIN\Administrators:(I)(F)
                                                                                        BUILTIN\Users:(I)(RX)

c:\ProgramData\Mudhook Marketing, Inc\SaferVPN\Diagnostics\Service\netfilter.rules.log NT AUTHORITY\SYSTEM:(I)(F)
                                                                                       BUILTIN\Administrators:(I)(F)
                                                                                       BUILTIN\Users:(I)(RX)

c:\ProgramData\Mudhook Marketing, Inc\SaferVPN\Diagnostics\Service\service.error.log NT AUTHORITY\SYSTEM:(I)(F)
                                                                                     BUILTIN\Administrators:(I)(F)
                                                                                     BUILTIN\Users:(I)(RX)

c:\ProgramData\Mudhook Marketing, Inc\SaferVPN\Diagnostics\Service\service.log NT AUTHORITY\SYSTEM:(I)(F)
                                                                               BUILTIN\Administrators:(I)(F)
                                                                               BUILTIN\Users:(I)(RX)

Successfully processed 4 files; Failed processing 0 files

C:\>_
```

Timeline

09–08–2020 — Vulnerability discovered

09–08–2020 — Notified the vendor via email (vendor replied to send the details of the vulnerability)

09–08–2020 — Sent the details of the vulnerability

16–08–2020 — Followed up the vendor (vendor did not respond)

30–08–2020 — Followed up the vendor again (vendor did not respond)

16–09–2020 — Vendor silently fixed the vulnerability and released a new version

17–09–2020 — Public disclosure

18–09–2020 — CVE Assigned CVE-2020-25744

Cve Dos Cybersecurity Mitre Vulnerability