HMA VPN 5.3 Unquoted Service Path

2022.02.22

Credit: **Saud Alenazi (https://cxsecurity.com/author/Saud+Alenazi/1/)**

Risk: **Medium**

Local: **Yes**

Remote: **No**

CVE: **N/A**

CWE: **N/A**

```
# Exploit Title: HMA VPN 5.3 - Unquoted Service Path
# Date: 18/02/2022
# Exploit Author: Saud Alenazi
# Vendor Homepage: https://www.hidemyass.com/
# Software Link: https://www.hidemyass.com/en-us/downloads
# Version: 5.3.5913.0
# Tested: Windows 10 Pro x64 es


C:\Users\saudh>sc qc HmaProVpn
[SC] QueryServiceConfig SUCCESS
```

```
SERVICE_NAME: HmaProVpn
        TYPE               : 20  WIN32_SHARE_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : "C:\Program Files\Privax\HMA VPN\VpnSv
c.exe"
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : HMA VPN
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem


#Exploit:

A successful attempt would require the local user to be able to ins
ert their code in the system root path undetected by the OS or othe
r security applications where it could potentially be executed duri
ng application startup or reboot. If successful, the local user's c
ode would execute with the elevated privileges of the application.
```

See this note in RAW Version (https://cxsecurity.com/ascii/WLB-2022020111)

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)