CVE-2020-0601 - CryptoAPI

Die Schwachstelle in der CryptoAPI wird bei Microsoft unter diesem Link behandelt.

CVE-2020-0601 | Windows CryptoAPI Spoffing Vulnerability

Bei der Schwachstelle geht es um eine Programmbibliothek (DLL) namens Crypt32.dll. Dieses befindet sich im Verzeichnis C:\Windows\System32.

Security Update Guide:

https://portal.msrc.microsoft.com/en-us/security-guidance

Ein Angreifer kann diese Schwachstelle ausnutzen, um z.B. ausführbare Dateien mit einem gefälschten Zertifikat zur Code-Signierung zu signieren, ohne dass das Betriebssystem es mitbekommt.

Betroffen sind folgende Plattformen:

- Windows 10
- Windows Server 2016
- Windows Server 2019

Die Schwere der Schwachstelle wird als „Important" eingestuft.

Beeinträchtigungen:

Es können z.B. folgende Integritäten beeinträchtigt sein.

- HTTPS-Verbindungen
- Signierte .exe Dateien
- Signierte E-Mails oder Dateien

Folgende Cumulative Updates zum Schließen der Lücke stehen bereit:

- KB4528760 für Windows 10 v1909
- KB4534271 für Windows Server 2016
- KB4528760 für Windows Server 2019 v1909

Das Problem welches sich aus dieser Schwachstelle ergibt ist, dass ein Angreifer den verschlüsselten Datenverkehr mitlesen kann. Dazu wird die geglaubte sichere HTTPS-Verbindung aufgebrochen.

Microsoft setzt auf das CVD (Coordinated Vulnerability Disclosure) als bewährte Best Practise Methode zur Behebung von Sicherheitslücken. Hierbei handelt es sich um eine Partnerschaft verschiedener Sicherheitsforschern und Anbietern, die sich zum Ziel gemacht haben, Schwachstellen zu beseitigen bevor sie zur Bedrohung werden können.

https://www.microsoft.com/en-us/msrc/cvd

https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf

Aktuell soll es noch keine aktiven Angriffe geben, es stehen aber bereits mehrere *POCs zur Verfügung.

https://github.com/kudelskisecurity/chainoffools
https://github.com/ollypwn/cve-2020-0601

CVE-2020-0601 - CryptoAPI

Überprüfung:

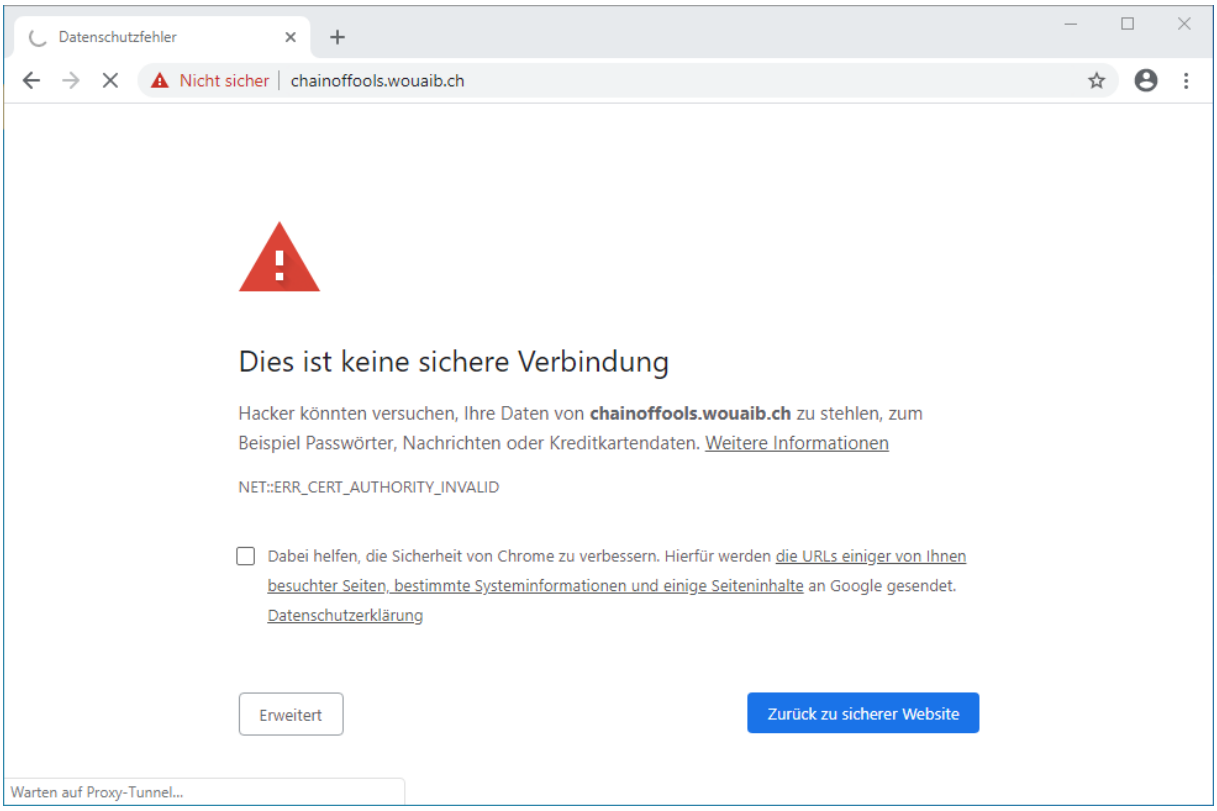
Mithilfe dieser Webseite soll sich prüfen lassen, ob ein System anfällig bzw. noch nicht gepatched wurde. Bitte mit Chrome oder dem IE/Edge testen, da der Mozilla Firefox über eine native Prüfmethode verfügt und das Ergebnis verfälscht wäre.

https://chainoffools.wouaib.ch/

Erscheint nach dem Aufruf folgender Hinweis, dann ist die Maschine nicht sicher und erkennt das gefälschte Zertifikat nicht.

Hello World!
This is a CryptoAPI CVE-2020-0601 POC by Kudelski Security!
Read our write-up on our Research blog!

Wenn das gefälschte Zertifikat erkannt wird, ist die Verbindung nicht sicher und es erscheint folgender Hinweis:



Der Test macht auf Maschinen hinter einem Proxy keinen Sinn, weil diese in der Regel das Zertifikat aufbrechen.

CVE-2020-0601 - CryptoAPI

***POC auf Github:**

CryptoAPI

CVE-2020-0601: Windows CryptoAPI Spoofing Vulnerability exploitation. More information in our blog post.

CA certificate

We used the USERTrust ECC Certification Authority

Key template:

```
$ openssl ecparam -name secp384r1 -genkey -noout -out p384-key.pem -param_enc
explicit
```

To generate a private key which match the public key certificate we used the script **gen-key.py** (works with Python 3.6 and above). Then to generate the rogue CA:

```
$ openssl req -key p384-key-rogue.pem -new -out ca-rogue.pem -x509 -set_serial
0x5c8b99c55a94c5d27156decd8980cc26
```

With "C = US, ST = New Jersey, L = Jersey City, O = The USERTRUST Network, CN = USERTrust ECC Certification Authority" parameters

The we generate the following private key and certificate:

```
openssl ecparam -name prime256v1 -genkey -noout -out prime256v1-privkey.pem

openssl req -key prime256v1-privkey.pem -config openssl.cnf -new -out
prime256v1.csr

openssl x509 -req -in prime256v1.csr -CA ca-rogue.pem -CAkey p384-key-rogue.pem -
CAcreateserial -out client-cert.pem -days 500 -extensions v3_req -extfile
openssl.cnf
```

CVE-2020-0601 - CryptoAPI

Empfohlenes Vorgehen:

Zuerst sollten alle Domain-Controller, Web-Server, DNS- und Proxy-Server aktualisiert werden, gefolgt von den Windows 10 Client-Systemen.

Jedes System sollte so eingestellt werden, dass es Zertifikate validiert und auch die Sperrlisten sollten erreichbar sein.

Zugriffe nach außen sollten eingeschränkt werden.