# گزارش آسيبپذيرى CVE-2020-0601

شرح آسیبپذیری در CryptoAPI ویندوز و نحوه رفع آن به زبان ساده



## شماره گزارش VU00301

بهمن ۱۳۹۸



🔜 تهران، آزادراه تهران ـ کرج، بلوار چوگان، روبروی شهرک آزادی، پردیس نوآوری شهید مقدم، واحد ۸





www.AmnBan.ir 🌐







### فهرست

ھرست۳	ė
- شروع ماجرا۴	١
۱- آسیبپذیری CVE-2020-0601 چه آثار مخربی دارد؟۴	٦
۲- آیا سیستم من آسیبپذیر است؟۲- آیا سیستم من آسیبپذیر است؟	IJ
۲-۲- روش برخط (Online)	
۲-۳- روش غیربرخط (Offline)	
۱- نحوه مقابله۱- نحوه مقابله.	F
۲-۲- روش اول - به روزرسانی خودکار (توصیه می شود)۸	
۲ <b>-۴-</b> روش دوم - به روزرسانی دستی:۸	
، بررسی نصب بودن به روزرسانی	2
۵-۱- روش اول۱۲	
۵-۲- روش دوم	
۵-۳- روش سوم	
۵-۴- روش چهارم (حرفهای)	



#### ۱- شروع ماجرا

در روزهای گذشته خبر آسیبپذیری با شناسه CVE-2020-0601 در سیستم عامل ویندوز ۱۰ و ویندوز سرور ۲۰۱۶ و ۲۰۱۹ یکی از اخبار جالب و بسیار نگران کننده بود. جالب از این جهت که این آسیبپذیری را اولین بار NSA اعلام کرد و نگران کننده از این جهت که NSA اعلام کرد! سازمانی که خود سابقه تاریکی در جاسوسی از شهروندان امریکایی و غیر امریکایی دارد این آسیبپذیری را اعلام کرد و احتمالاً به این دلیل است که NSA متوجه شده هکرهای سایر کشورها مانند روسیه یا چین هم از این آسیبپذیری استفاده میکنند و با اعلام آن سعی کرده در کار آنها اختلال ایجاد کند وگرنه NSA چندان خیر خواه امنیت دیگران نیست. در آسیبپذیری D-15M یا همان EternalBlue هم با اینکه NSA مدتها قبل آسیبپذیری را کشف کرده بود اما آن را اعلام نکرده بود و سالها از آن استفاده میکرد تا اینکه پس از نفوذ گروه Broker به Shadow Broker این مورد را منتشر کرد<sup>4</sup>.

در این گزارش به زبان ساده خطرات این آسیبپذیری، نحوه بررسی آسیبپذیر بودن سیستم و به روزرسانی آن را شرح خواهیم داد.

### ۲- آسیبپذیری **CVE-2020-0601** چه آثار مخربی دارد؟

این آسیبپذیری روی (Crypt32.dll) CryptoAPI است که ویندوز و برخی نرم افزارها از آن برای اعتبارسنجی گواهینامه با رمزنگاری منحنی بیضوی (Elliptic Curve) استفاده میکنند و میتواند منجر به جعل گواهینامه شود. دقت کنید که خود الگوریتم رمزنگاری منحنی بیضوی آسیبپذیر نیست و جزو امن ترین الگوریتمهای رمزنگاری دنیا است آسیبپذیری روی پیاده سازی آن است برای توضیحات بیشتر می توانید به اینجا مراجعه فرمایید. جعل گواهیهای رمزنگاری که در ارتباطات رمزشده استفاده میشود میتواند باعث حمله مرد میانی<sup>۳</sup> و شنود ارتباط رمزشده هم بشود<sup>ع</sup>. از طرفی بسیاری از برنامهها در ویندوز دارای امضای دیجیتال از طرف سازنده هستند (شکل ۱) به کمک ابزار <u>Sigcheck</u> هم میتوانید امضای دیجیتال برنامه ها را بررسی کنید. به عنوان مثلا خروجی بررسی برنامه پرکاربرد <u>Sigcheck</u> هم میتوانید امضای دیجیتال برنامه ها را بررسی کنید. به عنوان مثلا خروجی بررسی افزار از طرف یک سازنده معتبر مثلا Microsoft ایجاد شده است و فایلی که در اختیار ماست توسط فرد دیگری دستکاری نشده و همان فایلی سازنده است. فاجعه بزرگ اینجاست که بسیاری از آنتی ویروسها با دیدن امضای معتبر یک برنامه آن را اسکن نمیکنند و مهاجمان به کمک این آسیبپذیری میتوانند هر برنامه مخربی را امضا معتبر یک برنامه آن را اسکن نمیکنند و مهاجمان به کمک این آسیبپذیری میتوانند هر برنامه مخربی را امضا در نرم فراره این سازنده معتبر مانده است. فاری اینجاست که بسیاری از آنتی ویروسها با دیدن امضای معتبر یک برنامه آن را اسکن نمیکنند و مهاجمان به کمک این آسیبپذیری میتوانند هر برنامه مخربی را امضا در نرم افزارهایی ماننده معتبر مانده است. فاره نوان اجازه اجرا فقط به فایلهای دارای امضای معتبر داده شده توسط یک سازنده معتبر مانند از می میتوان هر فایل مخربی را در آن اجرا کرد.

https://media.defense.gov/2020/Jan/14/2002234275/-1/-1/0/CSA-WINDOWS-10-CRYPT-LIB-20190114.PDF

<sup>&</sup>lt;sup>r</sup> https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/

<sup>&</sup>lt;sup>r</sup> Man-in-the-Middle(MitM)

<sup>&</sup>lt;sup>+</sup> https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0601



Open File - Security Warning	Open File - Security Warning
The publisher could not be verified. Are you sure you want to run this software?	Do you want to run this file?
Name:         C:\GlobalSign\Unsigned\Untrusted.exe           Publisher:         Unknown Publisher           Type:         Application           From:         C:\GlobalSign\Unsigned\Untrusted.exe	Name:         C:\GlobalSign\Signed\CodeSigned.exe           Publisher:         GlobalSign_LTD           Type:         Application           From:         C:\GlobalSign\Signed\CodeSigned.exe
Run Cancel	Run Cancel
This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust <u>How can!</u> decide what software to run?	While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk2

شکل ۱- برنامه دارای امضای معتبر (راست) و برنامه با امضای نامعتبر (چپ)

C:\\	Vindows\System32\cmd.	exe			
Microso (c) 201	licrosoft Windows [Version 10.0.17763.615] (c) 2018 Microsoft Corporation. All rights reserved.				
D:\Dowr	D:\Downloads\Sigcheck>sigcheck64.exe C:\WINDOWS\system32\nslookup.exe				
Sigcheo Copyrio Sysinte	Sigcheck v2.73 - File version and signature viewer Copyright (C) 2004-2019 Mark Russinovich Sysinternals - www.sysinternals.com				
c:\win	Verified: Organing date. Publisher:	Signed Signed Wicrosoft Windows			
	Company: Description: Product: Prod version: File version: MachineType:	Microsoft Corporation nslookup Microsoft« Windows« Operating System 10.0.17763.292 10.0.17763.292 (WinBuild.160101.0800) 64-bit			

شکل ۲- بررسی امضای nslookup.exe

توجه شود که اگر ابزاری برای رمزنگاری خود از کتابخانههای خودش استفاده کند و از ویندوز کمک نگیرد این آسیبپذیری روی آن تاثیری نخواهد داشت مانند مرورگر Firefox (البته ممکن است آسیبپذیریهای دیگری داشته باشد!)



#### ۳- آیا سیستم من آسیبپذیر است؟

برای بررسی آسیب پذیر بودن یک سیستم دو راه وجود دارد<sup>ه</sup> روش برخط (Online) و غیربرخط (Offline).

#### -۱-۳ روش برخط (Online)

در این روش با مرورگر Edge یا Internet Explorer به وب سایت https://curveballtest.com/index.html رفته اگر مانند شکل ۳ پیام You Are Vulnerable را مشاهده کردید شما آسیب پذیر هستید. اگر بعد از نصب به روزرسانی مجدداً عبارت You Are Vulnerable را مشاهده کردید چند بار دکمه Ctrl+F5 را فشارید تا صفحه کامل Refresh شود اگر پیام شکل

۴ را دیدید به روزرسانی به درستی انجام شده است.



شکل ۳- پیام آسیب پذیر بودن

<sup>&</sup>lt;sup>a</sup> https://isc.sans.edu/diary/Summing+up+CVE-2020-0601%2C+or+the+Let%3Fs+Decrypt+vulnerability/25720





شکل ۴- پیام آسیب پذیر نبودن

۳-۳- روش غیربرخط (Offline)

در این روش <mark>این فایل</mark> را دانلود بفرمایید و از حالت فشرده خارج کنید (کلمه عبور curveball) است. روی فایل کلیک راست کنید و روی Properties کلید کنید در برگه Digital Signatures در وسط صفحه Microsoft Windows را انتخاب کنید و روی Details کلیک کنید اگر در پنجره بازشده عبارت This digital signature is OK را مشاهده کردید (شکل ۵) سیستم شما آسیب یذیر است.

ligital Signature Det	ails	?	×	Digital Signature Details	? ×
General Advanced				General Advanced	
This digita	l signature is OK.	1		A certificate chain processed, but certificate which is not trusted by	terminated in a root the trust provider.
Signer information	1			Signer information	
Name:	oft Windows Hardwa	are Compatibility Publish	er	Name: pft Windows Hardwa	re Compatibility Publisher
E-mail:	Not available			E-mail: Not available	
Signing time:	Friday, January 17	, 2020 3:29:48 AM		Signing time: Friday, January 17,	2020 3:29:48 AM
Countersignature	s	View Certificat	e	Countersignatures	View Certificate
Name of signer	: E-mail address:	Timestamp		Name of signer: E-mail address:	Timestamp
Symantec Time	Not available	Friday, January 17,		Symantec Time Not available	Friday, January 17,
		Details			Details
			ОК	1	OK

شکل ۵- سیستم ایمن (راست) سیستم آسیب پذیر (چپ)



#### ۴- نحوه مقابله

برای مقابله با این آسیبپذیری باید ویندوز خود را طبق یکی از روشهای زیر به روز رسانی کنید.

#### ۱-۴- روش اول \_ به روزرسانی خودکار (توصیه می شود)

سیستم خود را به اینترنت متصل کنید و در منوی استارت ویندوز update را تایپ کنید و روی windows update و در صفحه بازشده Check for updates (شکل ۶) کلیک کنید و مدتی طولانی منتظر بمانید تا ویندوز شما آپدیت شود و درنهایت سیستم را Restart کنید و دوباره آسیب پذیر بودن سیستم خود را بررسی کنید.



شکل ۶- شروع بروزرسانی ویندوز

۲-۴- روش دوم \_ به روزرسانی دستی:

اگر به هر دلیلی امکان به روزرسانی خودکار برای شما وجود ندارد از این روش استفاده کنید.

ابتدا با نوشتن winver در run یا منو استارت ویندوز ۱۰ نسخه دقیق ویندوز را تعیین کنید مانند شکل ۷ که در این مثلا ویندوز ۱۸۰۹ است.



About Windows	×
Windows10	
Microsoft Windows	
Version 1809 (OS Build 17763.615)	
© 2018 Microsoft Corporation. All rights reserved.	
The Windows 10 Education operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries/regions.	
This product is licensed under the <u>Microsoft Software License</u> Terms to:	
Windows User	
OK	

شكل ٧-تعيين نسخه ويندوز

همچنین باید ۳۲ یا ۶۴ بیتی بودن ویندوز خود را با کلیک راست روی This PC و انتخاب Properties و مشاهده ۳۲ یا ۶۴ بیتی بودن در صفحه باز شده تعیین کنید (شکل ۸).



شکل ۸- تعیین ۳۲ یا ۶۴ بیتی بودن ویندوز



پس از تعیین نسخه دقیق ویندوز به <u>صفحه توضیحات آسیبپذیری بروید</u> و در بخش Security Updates متناسب با نسخه ویندوز خود آپدیت مناسب را انتخاب کنید و با کلیک روی Security Update به صفحه دانلود به روزرسانی بروید (شکل ۹).

Security Updates	Security Updates CVSS Score					
Security Updates						
To determine the support life cycle for your software version or edition, see the Microsoft Support Lifecycle.						
Product 🔺		Platform	Article	Download		
Windows 10 for 32-bit S	ystems		4534306	Security Update		
Windows 10 for x64-bas	ed Systems		4534306	Security Update		
Windows 10 Version 160	7 for 32-bit Systems		4534271	Security Update		
Windows 10 Version 160	7 for x64-based Systems		4534271	Security Update		
Windows 10 Version 170	9 for 32-bit Systems		4534276	Security Update		
Windows 10 Version 170	9 for ARM64-based Systems		4534276	Security Update		
Windows 10 Version 170	9 for x64-based Systems		4534276	Security Update		
Windows 10 Version 180	3 for 32-bit Systems		4534293	Security Update		
Windows 10 Version 180	3 for ARM64-based Systems		4534293	Security Update		
Windows 10 Version 180	3 for x64-based Systems		4534293	Security Update		
Windows 10 Version 180	9 for 32-bit Systems		4534273	Security Update		
Windows 10 Version 180	9 for ARM64-based Systems		4534273	Security Update		
Windows 10 Version 180	9 for x64-based Systems		4534273	Security Update		
Windows 10 Version 190	3 for 32-bit Systems		4528760	Security Update		
Windows 10 Version 190	3 for ARM64-based Systems		4528760	Security Update		

شکل ۹- انتخاب آپدیت مناسب

در صفحه دانلود بازهم متناسب با نسخه ویندوز خود روی دکمه Download کلیک کنید (شکل ۱۰).



Search results for "KB4534273"						
lates: 1 - 4 of 4 (page 1 of 1)						🔶 Previous   1
Title	Products	Classification	Last Updated	Version	Size	
2020-01 Cumulative Update for Windows 10 Version 1809 for x86-based Systems (KB4534273)	Windows 10	Security Updates	1/13/2020	n/a	131.0 MB	Download
2020-01 Cumulative Update for Windows 10 Version 1809 for ARM64-based Systems (KB4534273)	Windows 10	Security Updates	1/13/2020	n/a	308.9 MB	Download
2020-01 Cumulative Update for Windows Server 2019 for x64-based Systems (KB4534273)	Windows Server 2019	Security Updates	1/13/2020	n/a	281.4 MB	Download
2020-01 Cumulative Update for Windows 10 Version 1809 for x64-based Systems (KB4534273)	Windows 10	Security Updates	1/13/2020	n/a	281.4 MB	Download
2020-01 Cumulative Update for Windows Server 2019 for x64-based Systems (KB4534273) 2020-01 Cumulative Update for Windows 10 Version 1809 for x64-based Systems (KB4534273)	Server 2019 Windows 10	Updates Updates	1/13/2020 1/13/2020	n/a n/a	281.4 MB 281.4 MB	Downlo

📦 Microsoft Update Catalog - Mozilla Firefox	_		>
	··· (	פ ל	-
Download			
Download Updates			
2020-01 Cumulative Update for Windows 10 Version 1809 for x64-based Systems (	KB453427	3)	
windows10.0-kb4534273-x64_74bf76bc5a941bbbd0052caf5c3f956867e1de38.msu			

#### شکل ۱۱- لینک دانلود آپدیت

پس از دانلود، فایل دریافتی که با نامی مشابه windows10.0-kb4534273-xxxxxxxxxx.msu است را اجرا کنید و روی Yes کلیک کنید تا نصب آپدیت آغاز شود. در پایان پیام شکل ۱۲ نمایش داده میشود و روی Restart Now کلید کنید تا نصب تکمیل شود.



K Dowr	nload and Install Updates	×
<b>\$</b>	Installation complete You must restart your computer for the updates to take effect.	
	Restart Now Close	se

شکل ۱۲- پایان نصب آپدیت

#### ۵- بررسی نصب بودن به روزرسانی

برای بررسی آسیبپذیر بودن سیستم میتوانید با روشهای گفته شده در بخش آیا سیستم من آسیبپذیر است؟ عمل کنید یا با روشهای زیر از نصب به روزرسانی اطمینان حاصل کنید.

#### ۵-۱- روش اول

فایل نصب آپدیت را دوباره اجرا کنید اگر نصب باشد به شما پیام شکل ۱۳ نمایش داده میشود.



شکل ۱۳- پیام نصب بودن آپدیت



#### ۵-۲- روش دوم

برای بررسی نصب بودن به روزرسانی روی یک سیستم update history را در منو استارت ویندوز تایپ کنید و در برگه View update history به دنبال نام آن مثلاً kb4534273 بگردید (شکل ۱۴) توجه داشته باشید که بسته به نسخه ویندوز ممکن است نام بهروزرسانی فرق کند، مثلاً برای ویندوز 1903 نام به روزرسانی KB4528760 است این نام را در ابتدای نام فایل به روزرسانی دانلود شده می توانید ببینید در جدول ۱ نام آپدیتها بر اساس نسخه ویندوز آورده شده است.

☆ View update history
Uninstall updates
Recovery options
Update history $\checkmark$ Feature Updates (1)
Feature update to Windows 10 (business editions), version 1809, en-us Successfully installed on 1398/01/17
See what's new in this update
$\sim$ Quality Updates (50)
Security Update for Windows (KB4534273) Successfully instance on 1556/10/30
2019-07 Cumulative Update for .NET Framework 3.5, 4.7.2, 4.8 for Windows 10 Version 1809 for Successfully installed on 1398/04/23
2019-07 Cumulative Update for Windows 10 Version 1809 for x64-based Systems (KB4507469)

شکل ۱۴- بررسی نصب آپدیت

#### جدول ۱- جدول نام آپدیتها بر اساس نسخه ویندوز

Windows Version	KB Name
10-LTSB	KB4534306
10-1607, Server2016	KB4534271
10-1709	KB4534276
10-1803, Server2016-1803	KB4534293
10-1809, Server1909	KB4534273
10-1903, Server1903, 10-1909, Server1909	KB4528760



#### ۵-۳- روش سوم

در منوی استارت appwiz.cpl را تایپ کنید و آن را اجرا نمایید در سمت چپ روی View installed updates کلیک کنید در این صفحه دنبال آپدیت بگردید، از قسمت جستجوی بالا هم میتوانید کمک بگیرید (شکل ۱۵).

🐼 kb4534273 - Installed Updates - 🗆 🗙									
← → ✓ ↑ 🐼 → Control Panel → Programs → Programs and Features → Installed Updates 🗸 🖑 kb4534273									
	Control Panel Home	trol Panel Home Uninstall an update							
	Uninstall a program	To uninstall an update, select it from the list and then click Uninstall or Change.							
9	Turn Windows features on or								
	off	Organize 🔻					?		
	Install a program from the network	Name	Program	Version	Pu	ublisher			
	2 ->	Microsoft Windows (1)  Security Update for Microsoft Windows (KB4534273)	Microsoft Windows		м	licrosoft (	Corpora		

شکل ۱۵-بررسی نصب آپدیت روش دوم

#### ۵-۴- روش چهارم (حرفهای)

در powershell دستور Get-HotFix −Id با نام مناسب KB ( طبق جدول ۱) را وارد کنید اگر آپدیت نصب شده باشد خروجی باید به شکل ۱۶ باشد وگرنه پیام خطا نمایش داده میشود.

🛛 🔀 Windows	PowerShell										
Windows PowerShell Copyright (C) Microsoft Corporation. All rights reserved.											
PS C:\Users\Imp_> Get-HotFix -Id kb4534273											
Source	Description	HotFixID	InstalledBy	InstalledOn							
	Security Update	KB4534273	::::: <b>:</b>	1/20/2020 12:00:00							

شکل ۱۶- بررسی نصب با Powershell

تا آسیبپذیری جدید بدرود! 🕲

## درّباره ما:

گروه امنیت سایبری امنبان به همت جمعی از فارغ التحصیلان دانشگاه صنعتی شریف در سال ۱۳۹۷ با هدف آگاهی رسانی، تحقیق و پژوهش در جهت ارتقای امنیت سایبری کشور تشکیل شد. فعالیت این گروه به صورت رسمی از سال ۱۳۹۸ با ثبت شرکت امنبان فناوریهای پیشرفته شریف با شماره ثبت مرکت امنبان فناوریهای پیشرفته شریف با شماره ثبت ادامه یافت. همچنین مجموعه امنبان با کد عضویت ۲۱۰۱۳۸۸ عضو نظام صنفی رایانهای استان تهران میباشد.

YBER SECURITY GROUI

## تماس با ما؛



www.AmnBan.ir 🌐