گزارش آسیب‌پذیری CVE-2020-0601

شرح آسیب‌پذیری در CryptoAPI ویندوز

و نحوه رفع آن به زبان ساده

شماره گزارش VU00301

بهمن ۱۳۹۸

گروه امنیت سایبری امن‌بان
AMN BAN
CYBER SECURITY GROUP

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

۰۲۱ - ۲۸۴۲۴۴۶۳

www.AmnBan.ir

بسم الله الرحمن الرحیم

AMN BAN

گروه امنیت سایبری امن‌بان

گروه امنیت سایبری
امن‌بان
AMN BAN
CYBER SECURITY GROUP

فهرست

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[۱] 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 MS17-10 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 Shadow Brokers به NSA این مورد را منتشر کرد[۲].

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 CryptoAPI (Crypt32.dll) 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[۳] و شنود ارتباط رمزشده هم بشود[۴]. از طرفی بسیاری از برنامه‌ها در ویندوز دارای امضای دیجیتال از طرف سازنده هستند (شکل ۱) به کمک ابزار Sigcheck هم می‌توانید امضای دیجیتال برنامه ها را بررسی کنید. به عنوان مثلا خروجی بررسی برنامه پرکاربرد nslookup روی این سیستم به شکل ۲ است. این امضای دیجیتال نشان دهنده این است که نرم 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 شده توسط یک سازنده معتبر مانند Microsoft نشان دهند! حتی فایل‌های Macro در نرم افزارهایی مانند Word هم ار این قاعده مستثنا نیستند و اگر در تنظیمات این نرم افزار اجازه اجرا فقط به فایل‌های دارای امضای معتبر داده شده باشد اکنون با این آسیب‌پذیری می‌توان هر فایل مخربی را در آن اجرا کرد.

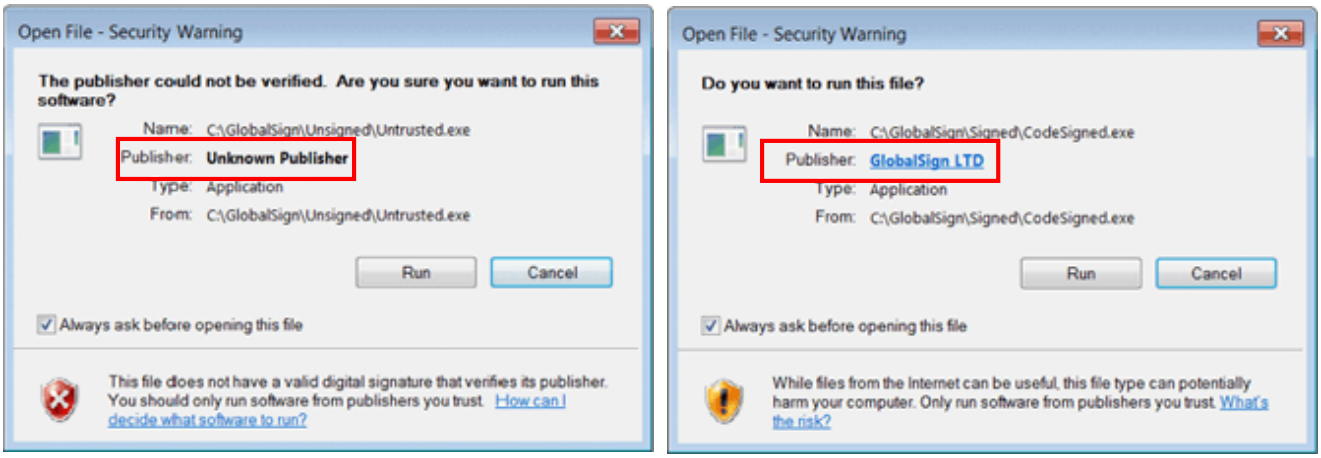
---

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

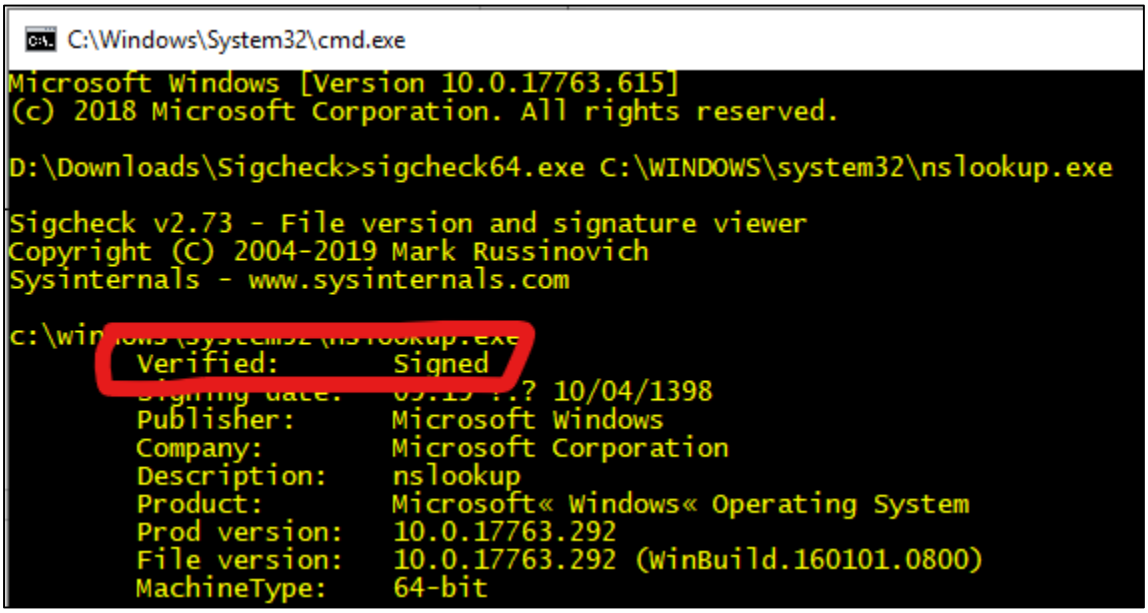
[۲] https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/

[۳] Man-in-the-Middle(MitM)

[۴] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0601



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



شکل ۲- بررسی امضای **nslookup.exe**

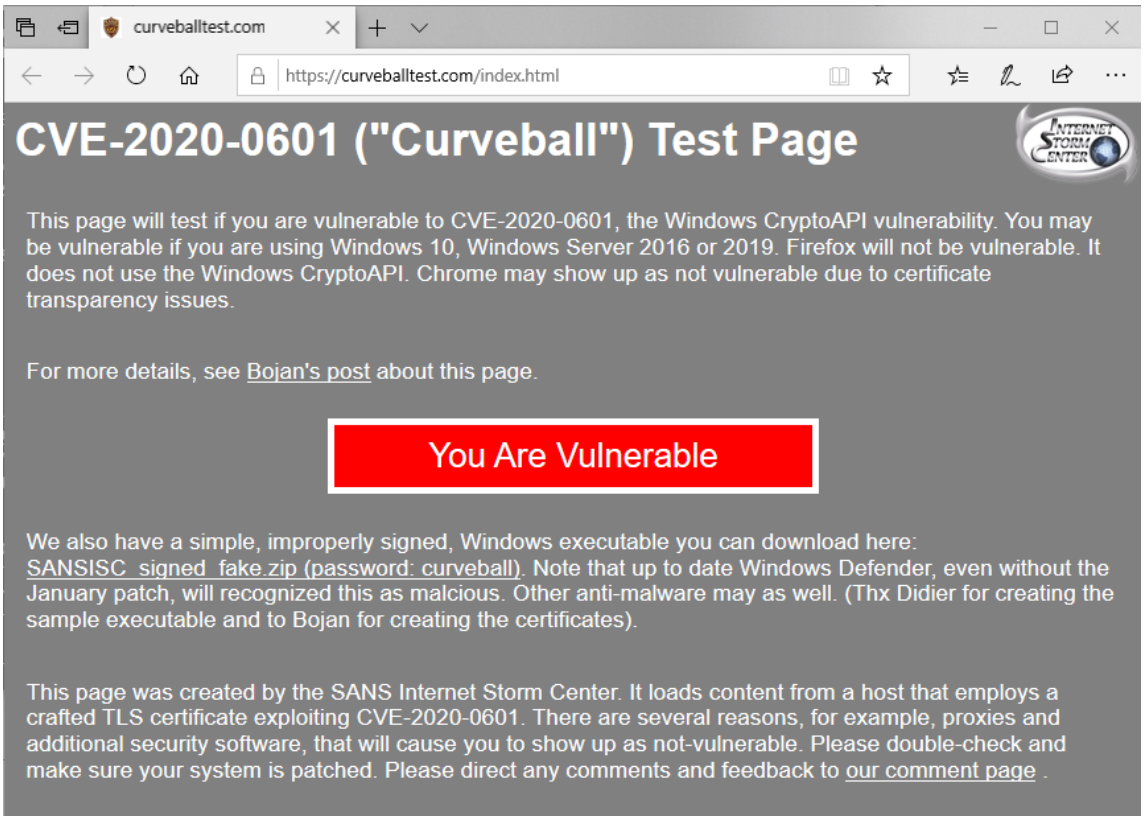
توجه شود که اگر ابزاری برای رمزنگاری خود از کتابخانه‌های خودش استفاده کند و از ویندوز کمک نگیرد این آسیب‌پذیری روی آن تاثیری نخواهد داشت مانند مرورگر Firefox (البته ممکن است آسیب‌پذیری‌های دیگری داشته باشد!)

۳- آیا سیستم من آسیب‌پذیر است؟

برای بررسی آسیب پذیر بودن یک سیستم دو راه وجود دارد[۵] روش برخط (Online) و غیربرخط (Offline).

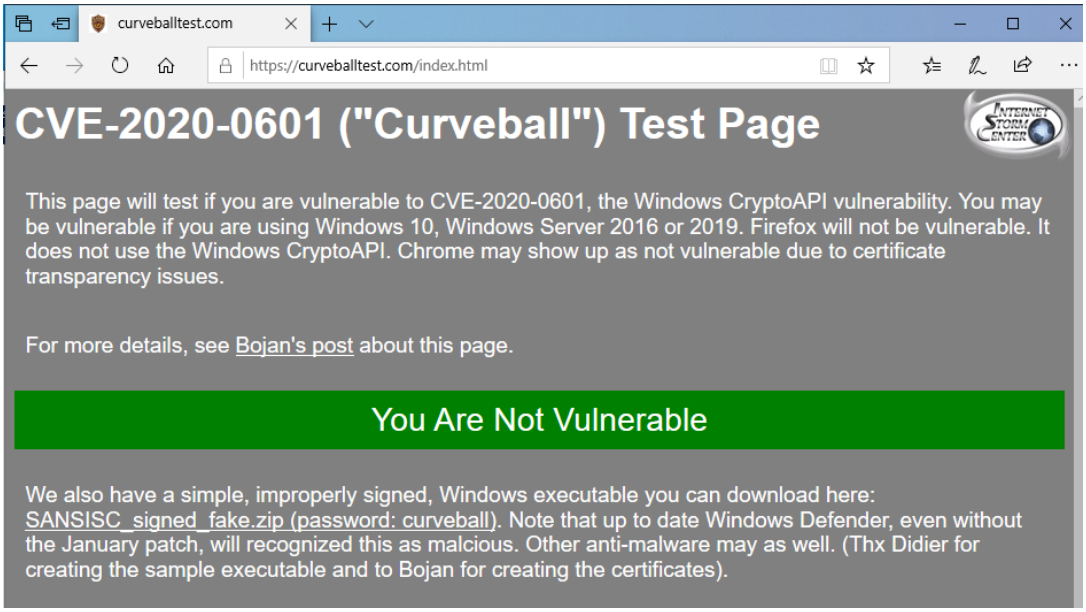
۳-۱- روش برخط (Online)

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

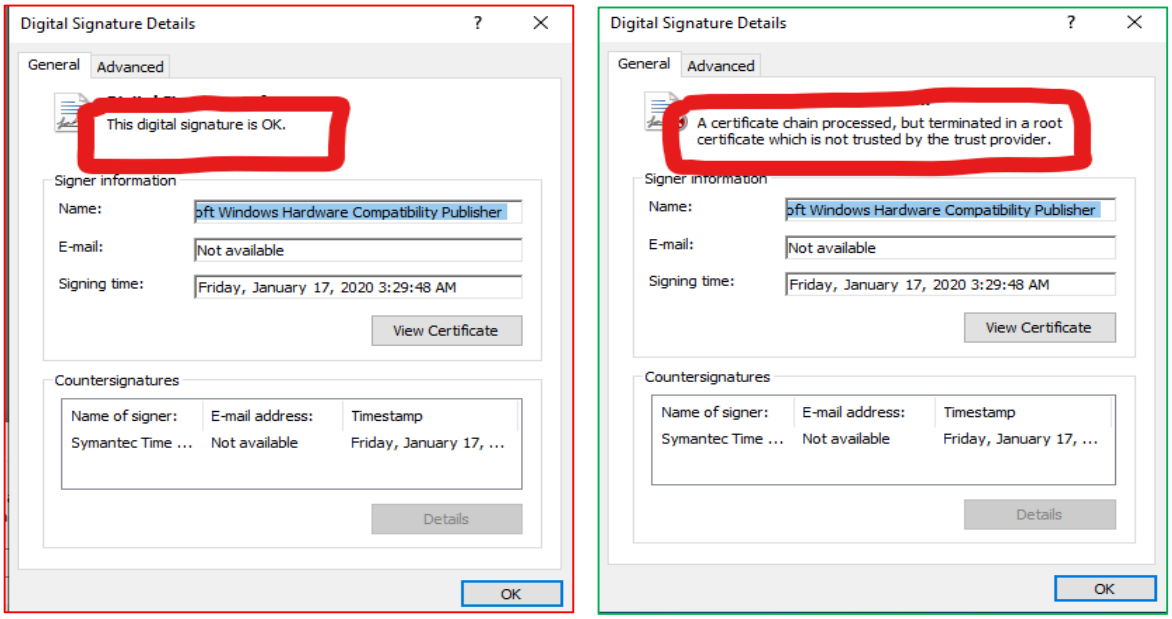
[۵] https://isc.sans.edu/diary/Summing+up+CVE-2020-0601%2C+or+the+Let%3Fs+Decrypt+vulnerability/25720



شکل ۴- پیام آسیب پذیر نبودن

۳-۲- روش غیربرخط (Offline)

در این روش این فایل 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 پذیر است.



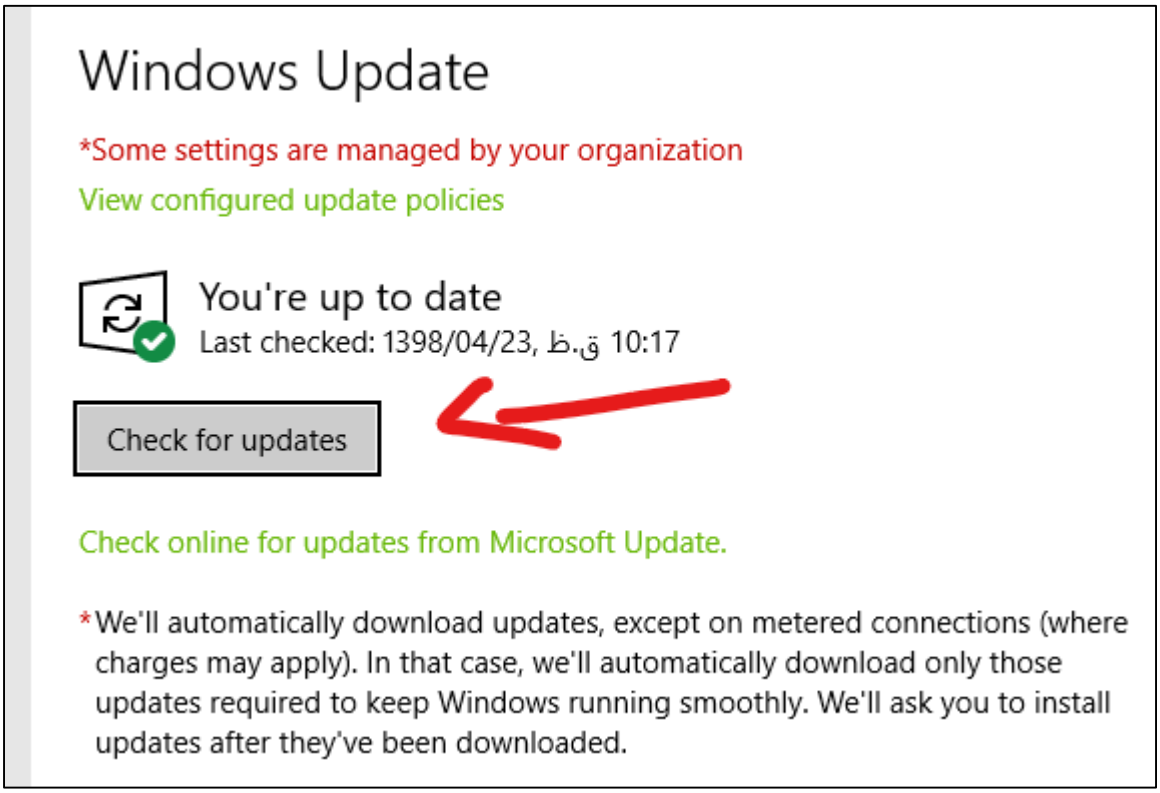
شکل ۵- سیستم ایمن (راست) سیستم آسیب پذیر (چپ)

۴- نحوه مقابله

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

۴-۱- روش اول ـ 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

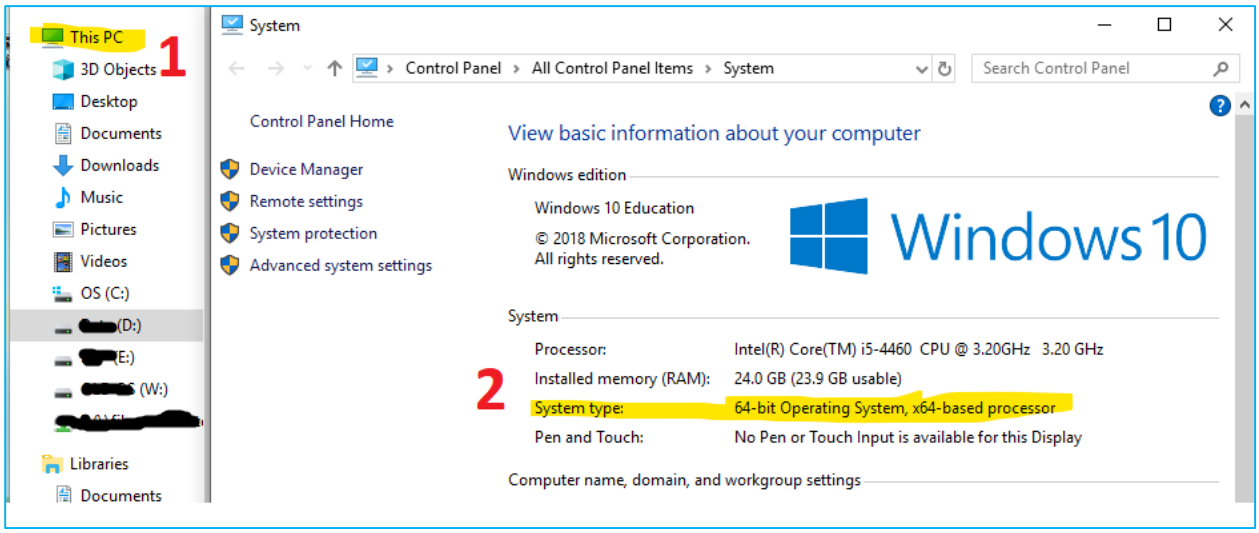
۴-۲- روش دوم ـ به روزرسانی دستی:

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.

شکل ۷-تعیین نسخه ویندوز

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 صفحه توضیحات آسیب‌پذیری بروید 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 | CVSS Score

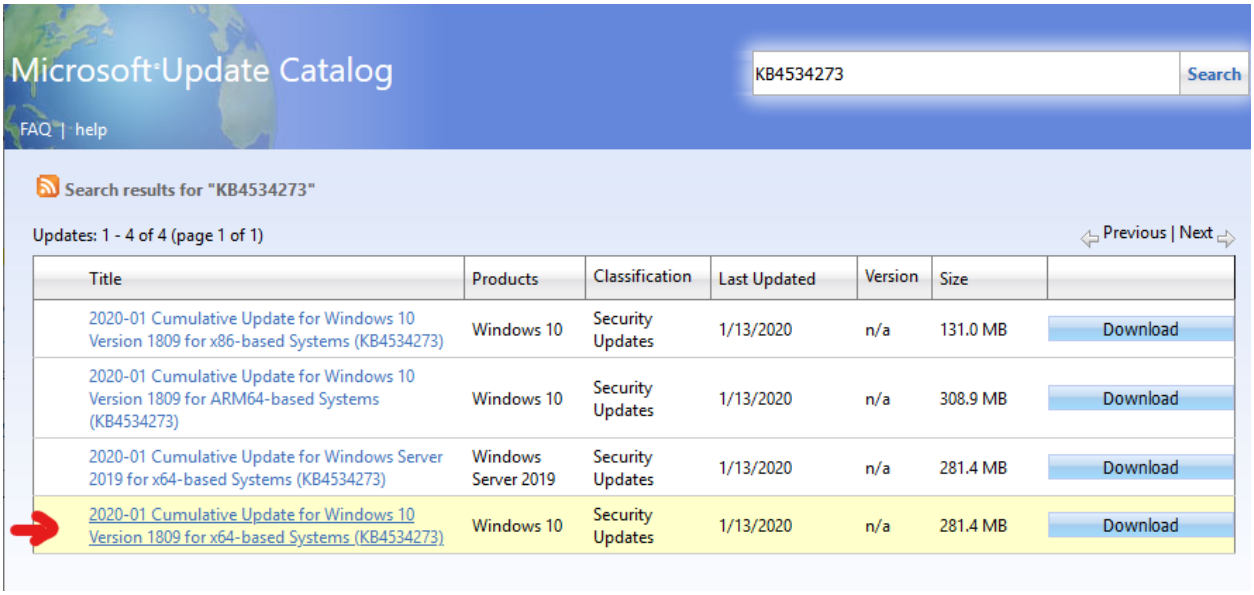
Security Updates

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 Systems		4534306	Security Update
Windows 10 for x64-based Systems		4534306	Security Update
Windows 10 Version 1607 for 32-bit Systems		4534271	Security Update
Windows 10 Version 1607 for x64-based Systems		4534271	Security Update
Windows 10 Version 1709 for 32-bit Systems		4534276	Security Update
Windows 10 Version 1709 for ARM64-based Systems		4534276	Security Update
Windows 10 Version 1709 for x64-based Systems		4534276	Security Update
Windows 10 Version 1803 for 32-bit Systems		4534293	Security Update
Windows 10 Version 1803 for ARM64-based Systems		4534293	Security Update
Windows 10 Version 1803 for x64-based Systems		4534293	Security Update
Windows 10 Version 1809 for 32-bit Systems		4534273	Security Update
Windows 10 Version 1809 for ARM64-based Systems		4534273	Security Update
Windows 10 Version 1809 for x64-based Systems		4534273	Security Update
Windows 10 Version 1903 for 32-bit Systems		4528760	Security Update
Windows 10 Version 1903 for ARM64-based Systems		4528760	Security Update

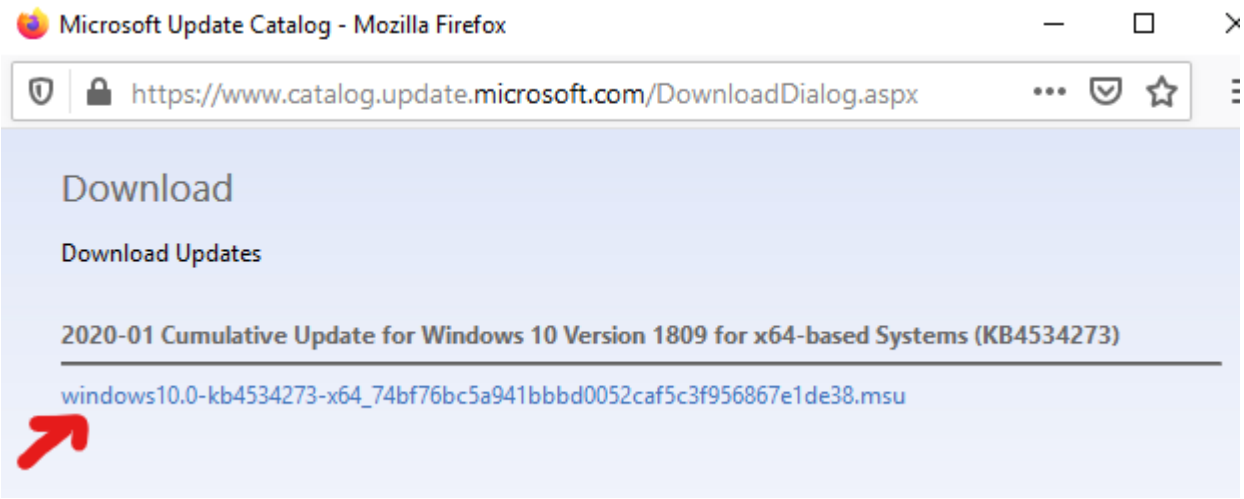
شکل ۹- انتخاب آپدیت مناسب

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



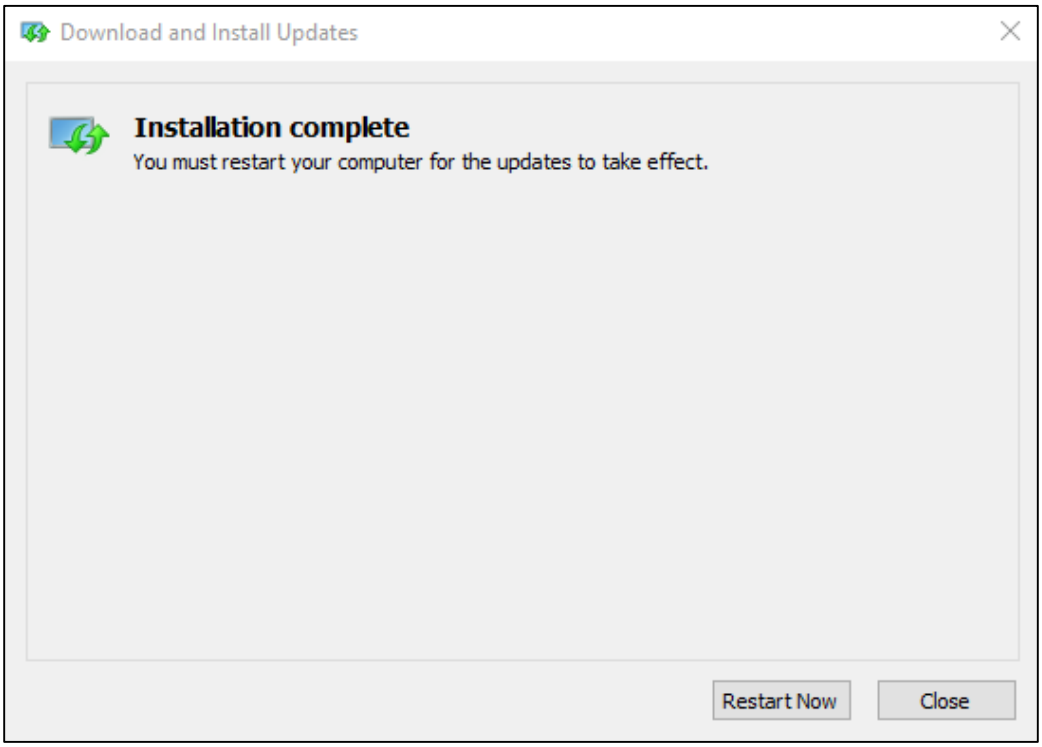
شکل ۱۰- صفحه دانلود آپدیت

در صفحه باز شده روی لینک آپدیت مورد نظر (شکل ۱۱) کلیک کنید تا دانلود فایل آغاز شود.



شکل ۱۱- لینک دانلود آپدیت

پس از دانلود، فایل دریافتی که با نامی مشابه windows10.0-kb4534273-xxxxxxxxxxxxxx.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.



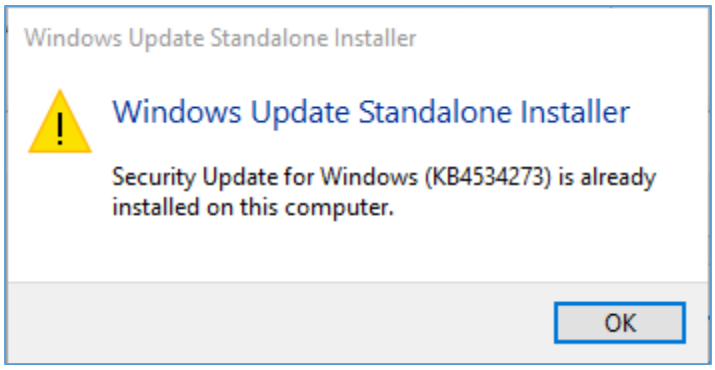
شکل ۱۲- پایان نصب آپدیت

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

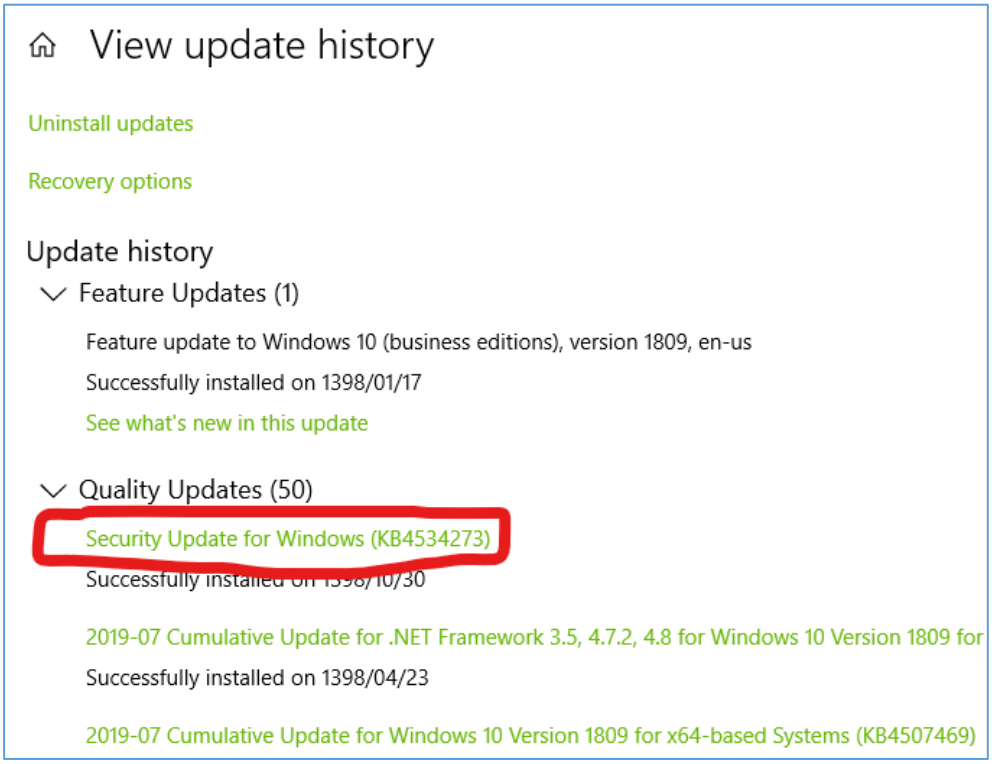
فایل نصب آپدیت را دوباره اجرا کنید اگر نصب باشد به شما پیام شکل ۱۳ نمایش داده می‌شود.



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.



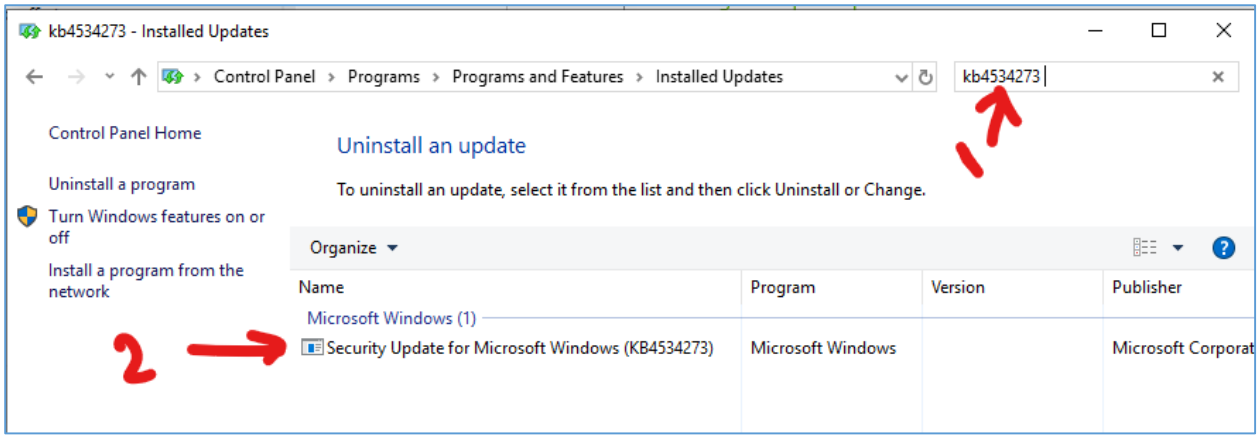
شکل ۱۴- بررسی نصب آپدیت

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

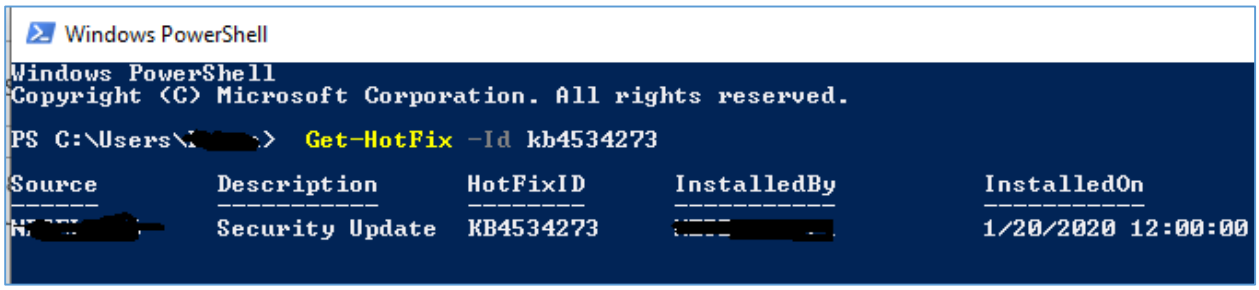
در منوی استارت appwiz.cpl را تایپ کنید و آن را اجرا نمایید در سمت چپ روی View installed updates کلیک کنید در این صفحه دنبال آپدیت بگردید، از قسمت جستجوی بالا هم می‌توانید کمک بگیرید (شکل ۱۵).



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.



شکل ۱۶- بررسی نصب با **Powershell**

تا آسیب‌پذیری جدید بدرود! ☺

درباره 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 ٥٤٤٨٩٤ و اخذ مجوز از مراجع ذی صلاح با نام تجاری امن‌بان ادامه یافت. همچنین مجموعه امن‌بان با کد عضویت ۲۱۰۱۳۸۸۰ عضو نظام صنفی رایانه‌ای استان تهران می‌باشد.

تماس با ما:

۰۲۱-۲۸۴۲۴۴۶۳

https://amnban.ir

mail@amnban.ir

شبکه‌های اجتماعی:

t.me/amnban

what.sapp.ir/AmnBAN

ble.ir/amnban

instagram.com/AmnBan