# گزارش آسیب‌پذیری CVE-2020-1472

## شرح آسیب‌پذیری ZeroLogon در Domain Controller

## و نحوه رفع آن

شماره گزارش VU00501

مهر ۱۳۹۹


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

## ۰- حق چاپ و نشر

این مستند گزارش آسیب‌پذیری است که توسط شرکت «امن‌بان فناوری‌شریف» تهیه شده است.

### رفع مسئولیت

شرکت «امن‌بان فناوری‌شریف» هیچگونه مسئولیتی در قبال سوء استفاده یا مشکلات استفاده از این گزارش ندارد و کلیه مسئولیت بر عهده استفاده کننده می‌باشد.

### کپی رایت

کلیه حقوق مادی و معنوی این مستند متعلق به شرکت «امن‌بان فناوری‌شریف» بوده و محفوظ می‌باشد. هرگونه نسخه برداری از قبیل رونوشت، ترجمه بخش یا بخش هایی از آن فقط با اخذ مجوز کتبی از «امن‌بان» امکان‌پذیر می‌باشد.

## ۱- شروع ماجرا

در روزهای گذشته خبر آسیب‌پذیری با شناسه CVE-2020-1472 و با نام ZeroLogon برای Domain Controller شبکه‌های ویندوزی توسط شرکت secura[۱] منتشر شد.

Domain Controller مهم‌ترین سرور در Active Directory است که وظیفه تعریف کاربران، احراز هویت و بسیاری از وظایف دیگر را به عهده دارد. آسیب‌پذیری ZeroLogon که دارای امتیاز CVSS 10 (بالاترین امتیاز ممکن) است که در ویندوزهای سرور از 2008R2 تا 2019 وجود دارد. بهره‌جویی[۲] این آسیب‌پذیری از راه دور قابل انجام است و نیاز به هیچ گونه احراز هویت ندارد. مهاجم به کمک این آسیب‌پذیری می‌تواند به دسترسی Domain Admin هم دست پیدا کند.

این آسیب پذیری در اثر ضعف در کانال امن ارتباطی Netlogon با Domain Controller وجود دارد.

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-2020-1472 چه آثار مخربی دارد؟

این آسیب‌پذیری چون به مهاجم دسترسی Domain Admin می‌دهد که دسترسی بسیار بالایی در شبکه‌های ویندوزی است و مهاجم به کمک این دسترسی عملاً می‌تواند علاوه بر سرور DC آسیب پذیر روی تمام سیستم‌های عضو دامنه نیز دسترسی پیدا کند، بسیار مخرب است.

## ۳- آیا سیستم من آسیب‌پذیر است؟

برای بررسی آسیب پذیر بودن یک سیستم، دو روش وجود دارد.

### روش اول : به کمک mimikatz

قابلیت تشخیص و بهره‌جویی ZeroLogon از نسخه 2.2.0-20200918 به mimikatz اضافه شده است. ابتدا جدیدترین نسخه mimikatz را از اینجا[۳] دانلود کنید. فایل دانلود شده احتمالاً توسط آنتی ویروس و مرورگر به عنوان فایل مخرب شناسایی می شود، نگران نباشید و آن را اجرا کنید.

در صفحه باز شده دستور زیر را وارد کنید.

```
lsadump::zerologon /target:dc1.test.local /ntlm /null /account:dc$
```

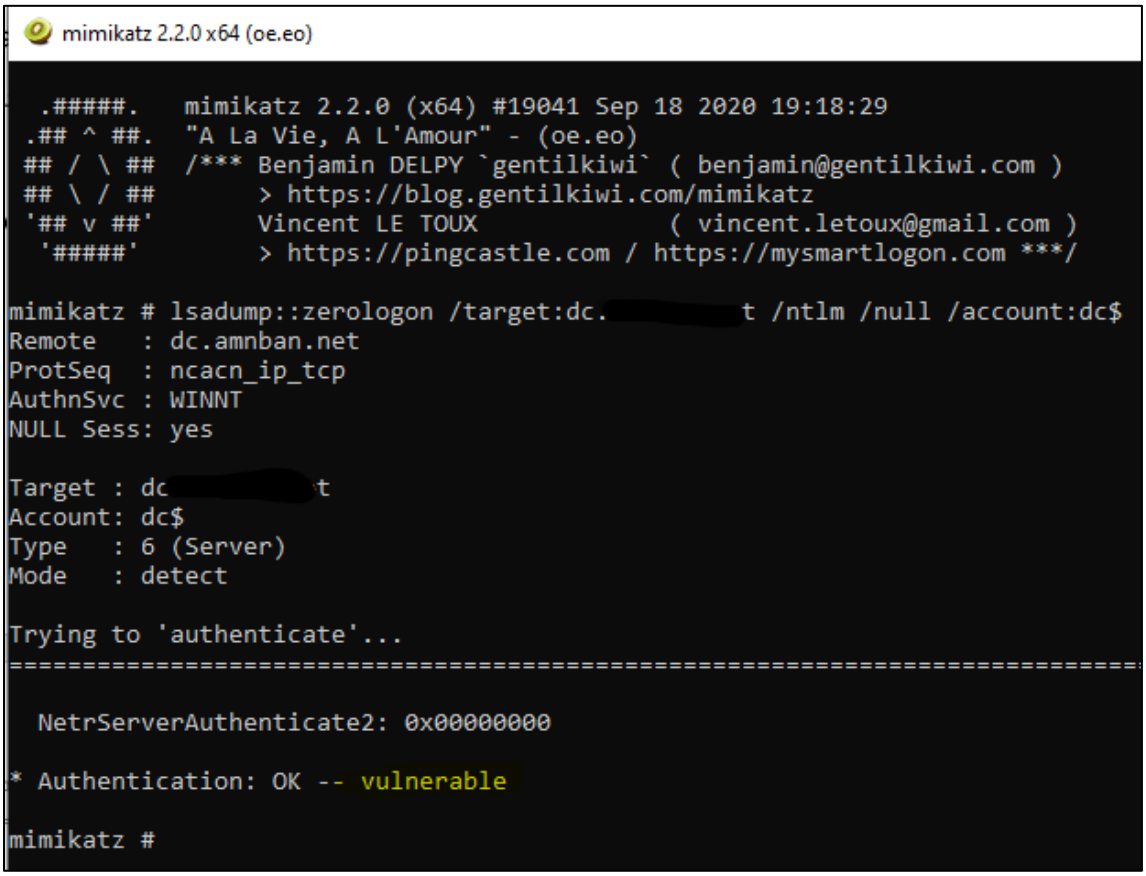
اگر خروجی زیر را مشاهده کردید DC شما آسیب پذیر است.

---

۱ https://www.secura.com/blog/zero-logon

۲ Exploit

۳ https://github.com/gentilkiwi/mimikatz/releases/

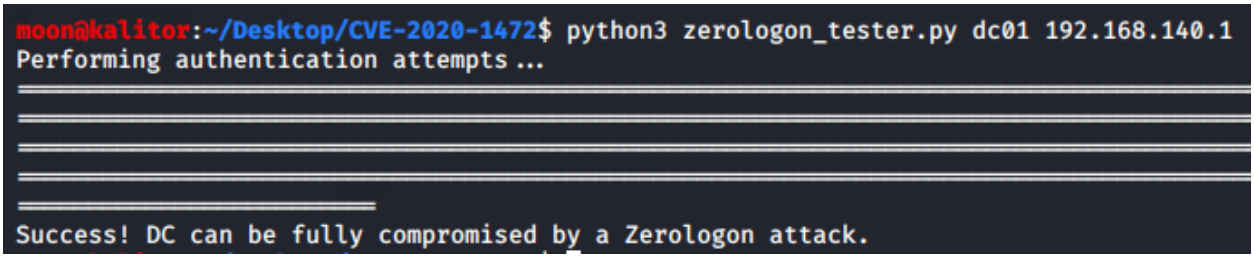



### روش دوم: به کمک اسکریپت پایتون

یک فایل پایتون توسط Secura در گیت هاب[۴] منتشر شده است که برای بررسی یک DC باید این فایل را روی یک سیستم لینوکسی (مثلا کالی لینوکس) به شکل زیر اجرا کنید.

phyton3 zerologon_tester.py DC_ NetBIOS_Name DC_ip_Address

در صورتی که سرور آسیب پذیر باشد پیامی مشابه تصویر زیر مشاهده خواهید کرد.



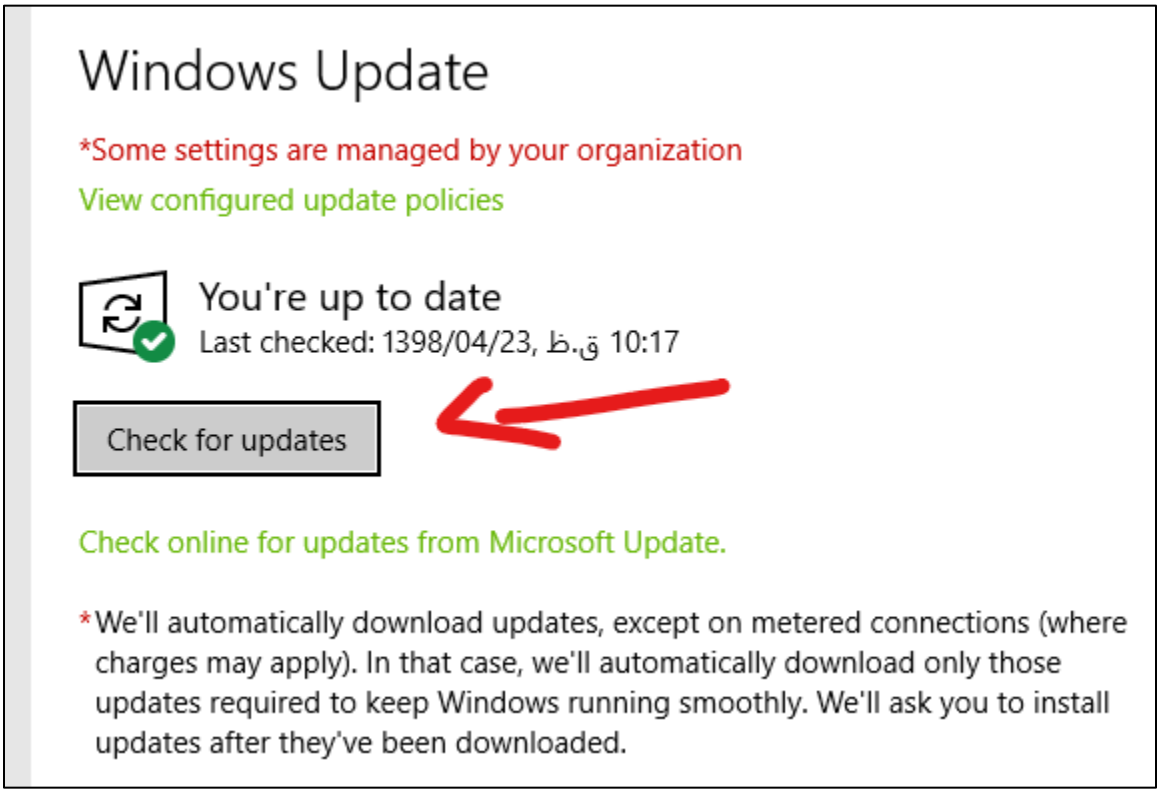

[۴] https://github.com/SecuraBV/CVE-2020-1472

## 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 ۱) کلیک کنید و مدت طولانی منتظر بمانید تا ویندوز شما آپدیت شود و درنهایت سیستم را Restart کنید.




شکل ۱- شروع بروزرسانی ویندوز

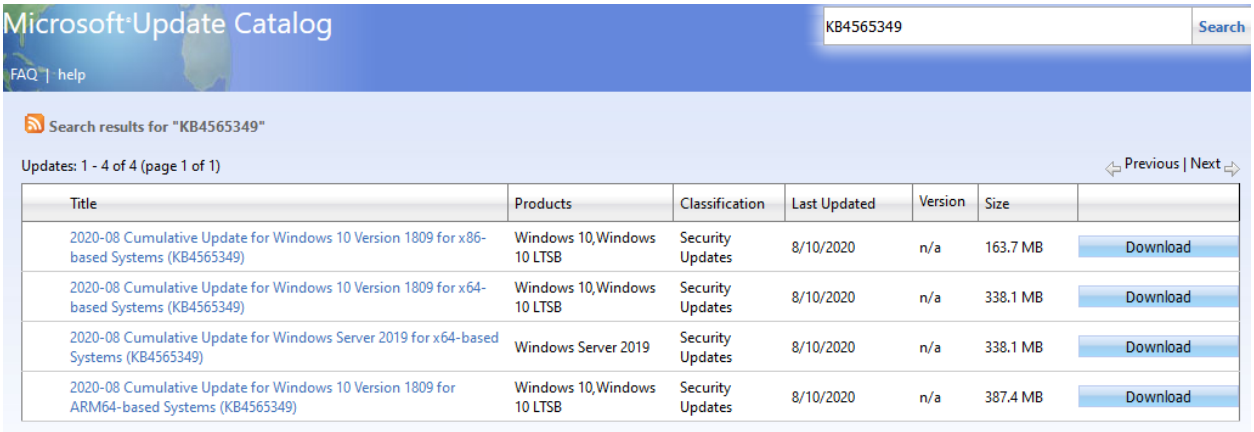
### ۴-۲- روش دوم ـ به روزرسانی دستی

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 نسخه دقیق ویندوز را تعیین کنید. پس از تعیین نسخه دقیق ویندوز به صفحه توضیحات آسیب‌پذیری بروید[۵] 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.

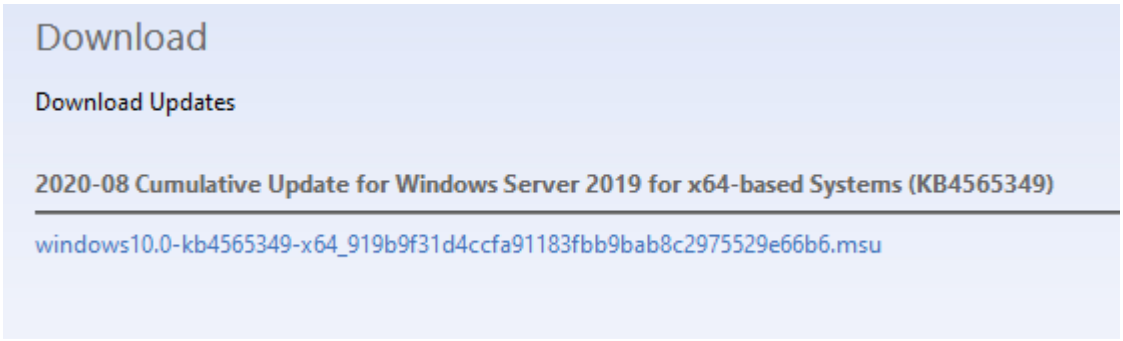
[۵] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472

در صفحه دانلود بازهم متناسب با نسخه ویندوز خود روی دکمه Download کلیک کنید (شکل ۲).



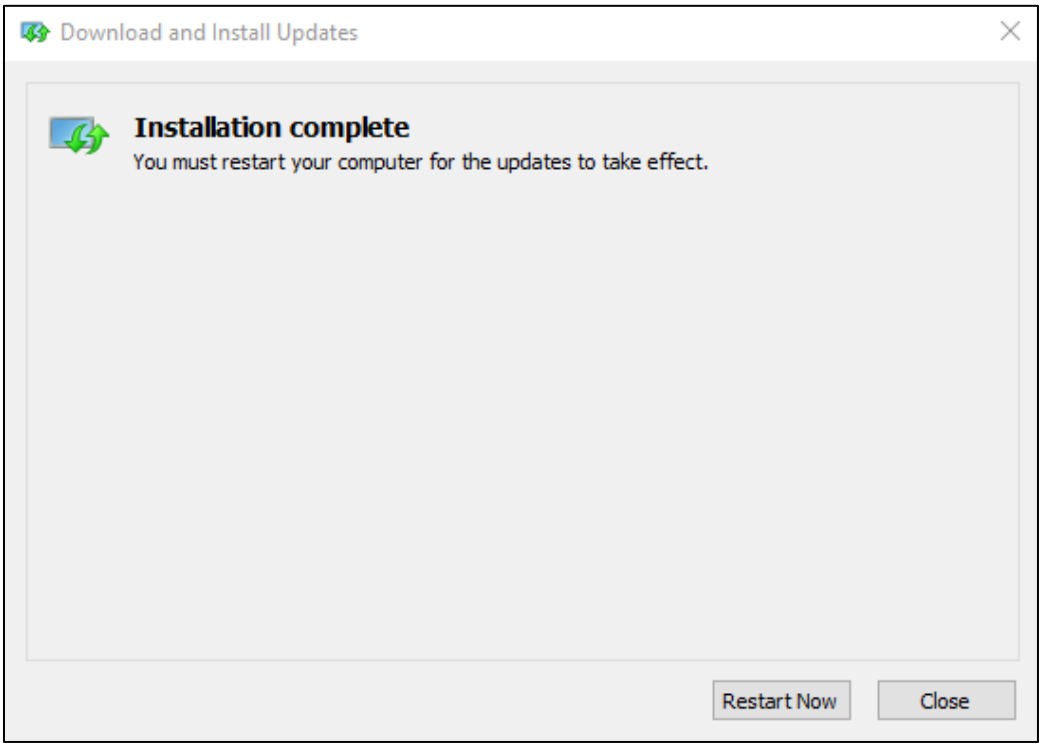

شکل ۲- صفحه دانلود آپدیت

در صفحه باز شده روی لینک آپدیت مورد نظر (شکل ۳) کلیک کنید تا دانلود فایل آغاز شود.




شکل ۳- لینک دانلود آپدیت

پس از دانلود، فایل دریافتی که با نامی مشابه windows10.0-kbxxx-xxxxxxxxxxxxxx.msu است را اجرا کنید و روی Yes کلیک کنید تا نصب آپدیت آغاز شود. در پایان پیام شکل ۴ نمایش داده می‌شود و روی Restart Now کلید کنید تا نصب تکمیل شود.



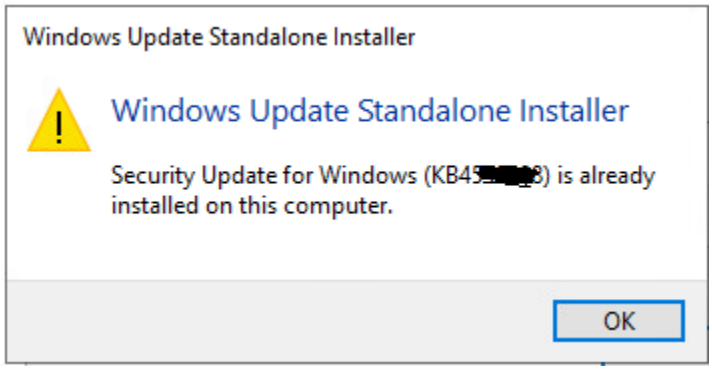

شکل ۴- پایان نصب آپدیت

## ۵- بررسی نصب بودن به روزرسانی

با روش‌های زیر از نصب به روزرسانی اطمینان حاصل کنید.

### ۵-۱- روش اول

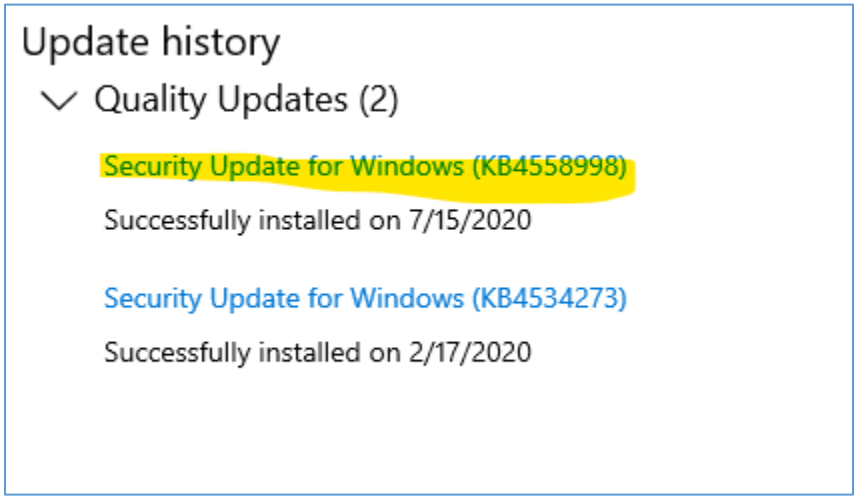
فایل نصب آپدیت را دوباره اجرا کنید اگر نصب باشد به شما پیام شکل ۵ نمایش داده می‌شود 😉.




شکل ۵- پیام نصب بودن آپدیت

### ۲-۵- 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 KB4565349 بگردید (شکل ۶). توجه داشته باشید که بسته به نسخه ویندوز ممکن است نام به‌روزرسانی متفاوت باشد. مثلاً برای ویندوز 2019 نام به روزرسانی KB4565503 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.



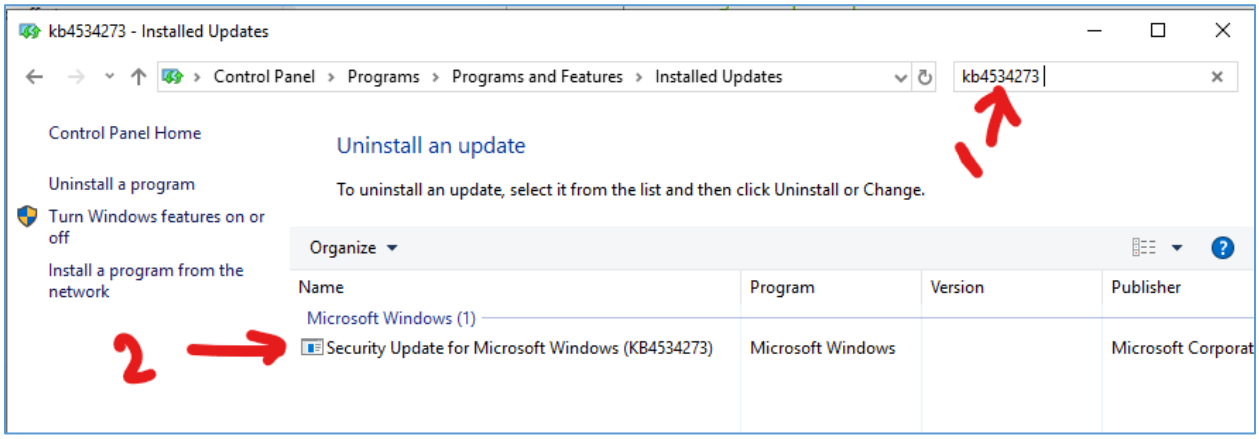

شکل ۶- بررسی نصب آپدیت

جدول ۱- جدول نام آپدیت‌ها بر اساس نسخه ویندوز

| Product | Platform | Article | Download | Impact | Severity | Supersedence |
|---|---|---|---|---|---|---|
| Windows Server, version 2004 (Server Core installation) | | ۴۵۶۶۷۸۲ | Security Update | Elevation of Privilege | Critical | ۴۵۶۵۵۰۳ |
| Windows Server, version 1909 (Server Core installation) | | ۴۵۶۵۳۵۱ | Security Update | Elevation of Privilege | Critical | ۴۵۶۵۴۸۳ |
| Windows Server, version 1903 (Server Core installation) | | ۴۵۶۵۳۵۱ | Security Update | Elevation of Privilege | Critical | ۴۵۶۵۴۸۳ |
| Windows Server 2019 (Server Core installation) | | ۴۵۶۵۳۴۹ | Security Update | Elevation of Privilege | Critical | ۴۵۵۸۹۹۸ |
| Windows Server 2019 | | ۴۵۶۵۳۴۹ | Security Update | Elevation of Privilege | Critical | ۴۵۵۸۹۹۸ |
| Windows Server 2016 (Server Core installation) | | ۴۵۷۱۶۹۴ | Security Update | Elevation of Privilege | Critical | ۴۵۶۵۵۱۱ |
| Windows Server 2016 | | ۴۵۷۱۶۹۴ | Security Update | Elevation of Privilege | Critical | ۴۵۶۵۵۱۱ |
| Windows Server 2012 R2 (Server Core installation) | | ۴۵۷۱۷۰۳<br>۴۵۷۱۷۲۳ | Monthly Rollup<br>Security Only | Elevation of Privilege | Critical | ۴۵۶۵۵۴۱ |
| Windows Server 2012 R2 | | ۴۵۷۱۷۰۳<br>۴۵۷۱۷۲۳ | Monthly Rollup<br>Security Only | Elevation of Privilege | Critical | ۴۵۶۵۵۴۱ |
| Windows Server 2012 (Server Core installation) | | ۴۵۷۱۷۳۶<br>۴۵۷۱۷۰۲ | Monthly Rollup<br>Security Only | Elevation of Privilege | Critical | ۴۵۶۵۵۳۷ |
| Windows Server 2012 | | ۴۵۷۱۷۳۶<br>۴۵۷۱۷۰۲ | Monthly Rollup<br>Security Only | Elevation of Privilege | Critical | ۴۵۶۵۵۳۷ |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) | | ۴۵۷۱۷۲۹<br>۴۵۷۱۷۱۹ | Monthly Rollup<br>Security Only | Elevation of Privilege | Critical | ۴۵۶۵۵۲۴ |
| Windows Server 2008 R2 for x64-based Systems Service Pack 1 | | ۴۵۷۱۷۲۹<br>۴۵۷۱۷۱۹ | Monthly Rollup<br>Security Only | Elevation of Privilege | Critical | ۴۵۶۵۵۲۴ |

### ۵-۳- روش سوم

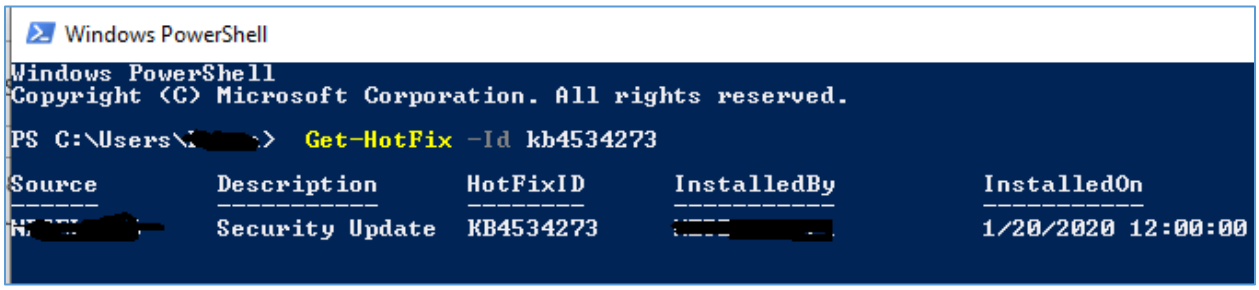
در منوی استارت appwiz.cpl را تایپ کنید و آن را اجرا نمایید در سمت چپ روی View installed updates کلیک کنید در این صفحه دنبال آپدیت بگردید، از قسمت جستجوی بالا هم می‌توانید کمک بگیرید (شکل ۷).




شکل ۷-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 ۸ باشد وگرنه پیام خطا نمایش داده می‌شود.




شکل ۸- بررسی نصب با **PowerShell**

## ۶- سوالات متداول

آیا این آسیب‌پذیری روی کلاینت‌ها هم تاثیری دارد؟

خیر، این آسیب‌پذیری فقط مربوط به سرور DC است.

**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 ۵٤٤٨٩٤ 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