

گزارش آسیب‌پذیری CVE-2021-31166

شرح آسیب‌پذیری CVE-2021-31166 و نحوه رفع آن



شماره گزارش VU00601

اردیبهشت ۱۴۰۰

تهران، آزاده تهران - کرج، بلوار چوگان، روبروی شهرک آزادی، پردیس نوآوری شهید مقدم، واحد ۸



۰۲۱ - ۲۸۴۲۴۴۶۳

www.AmnBan.ir



گروه امنیت سایبری

امن بان

AMN BAN
CYBER SECURITY GROUP



گروه امنیت سایبری
امن بان

AMN BAN

گروه امنیت سایبری امن بان

گروه امنیت سایبری

امن بان

AMN BAN

CYBER SECURITY GROUP





فهرست

فهرست	۳
۰- حق چاپ و نشر	۴
۱- شروع ماجرا	۵
۲- آسیب‌پذیری CVE-2021-31166 چه آثار مخربی دارد؟	۵
۳- آیا سیستم من آسیب‌پذیر است؟	۵
۴- نحوه مقابله	۶
۴-۱- روش اول - به‌روزرسانی خودکار (توصیه می‌شود)	۶
۴-۲- روش دوم - به‌روزرسانی دستی	۷
۵- بررسی نصب‌بودن به‌روزرسانی	۸
۵-۱- روش اول	۹
۵-۲- روش دوم	۹
۵-۳- روش سوم	۹
۵-۴- روش چهارم (حرفه‌ای)	۱۰



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 راییت

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.

Copyright

© Copyright 2020, AmnBan.ir

All rights reserved

All rights to this document belong to "AmnBan Fanavari Sharif" and are protected. All contents of this document are subject to change without notice. Copying and translating is only possible with the written permission of **AmnBan**.



۱- شروع ماجرا

در روزهای گذشته میکروسافت خبر آسیب‌پذیری با شناسه CVE-2021-31166 را برای سیستم‌عامل‌های ویندوزی منتشر کرد. آسیب‌پذیری CVE-2021-31166 که دارای امتیاز CVSS 9.8 (آسیب‌پذیری حیاتی) است در ویندوزهای سرور 2016 و ویندوز 10 که وب‌سروری بر آن‌ها در حال اجرا باشد، وجود دارد. CVE-2021-31166 به علت آسیب‌پذیری موجود در پشته پروتکل HTTP و مشکل استفاده از اشاره‌گر پس از آزادکردن آن رخ خواهد داد.

بهره‌جویی^۱ این آسیب‌پذیری از راه دور قابل انجام است و نیاز به هیچ گونه احراز هویت و تعامل کاربر ندارد. مهاجم به کمک این آسیب‌پذیری می‌تواند به صورت راه دور کد دلخواه موردنظر خود را اجرا کند.

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

۲- آسیب‌پذیری CVE-2021-31166 چه آثار مخربی دارد؟

از آنجا که با بهره‌جویی از این آسیب‌پذیری امکان اجرای کد از راه دور وجود دارد، مهاجم می‌تواند کد دلخواه خود را با سطح دسترسی سیستم بر سیستم قربانی اجرا کند. بنابراین این آسیب‌پذیری حیاتی می‌باشد.

۳- آیا سیستم من آسیب‌پذیر است؟

طبق گزارش میکروسافت این آسیب‌پذیری روی نسخه‌های 2004 و 20h2 از تمامی ویندوزهای سرور و ویندوز 10 که به‌روزرسانی مربوطه را نصب نکرده باشند، وجود دارد.

برای بررسی آسیب‌پذیر بودن یک سیستم، می‌توان از اسکریپت پایتونی که در گیت‌هاب^۲ منتشر شده استفاده کرد. برای اجرای این اسکریپت باید آدرس IP ویندوزی که وب‌سرور بر روی آن در حال اجرا است مشخص شده و به صورت زیر اسکریپت را با پایتون نسخه ۳ اجرا کنیم.

```
python3 cve-2021-31166.py --target=target_IP_address
```

در صورتی که ویندوز آسیب‌پذیر نباشد پیامی مشابه شکل ۱ مشاهده خواهید کرد.

```

[~/CVE-2021-31166-main]
$ python3 cve-2021-31166.py --target=192.168.20.210
<Response [200]>

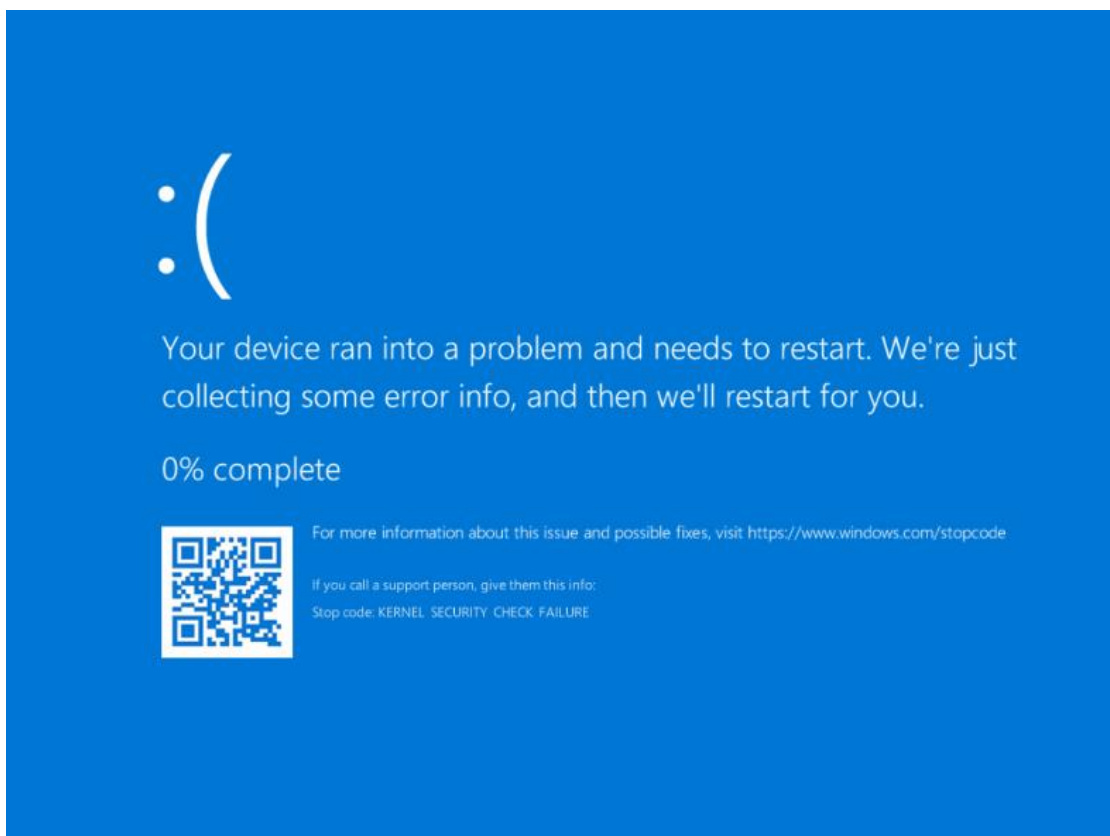
```

شکل ۱- بررسی آسیب‌پذیری سیستم

و اگر سیستم آسیب‌پذیر باشد Crash می‌کند (شکل ۲).

^۱ Exploit

^۲ <https://github.com/Overcl0k/CVE-2021-31166>



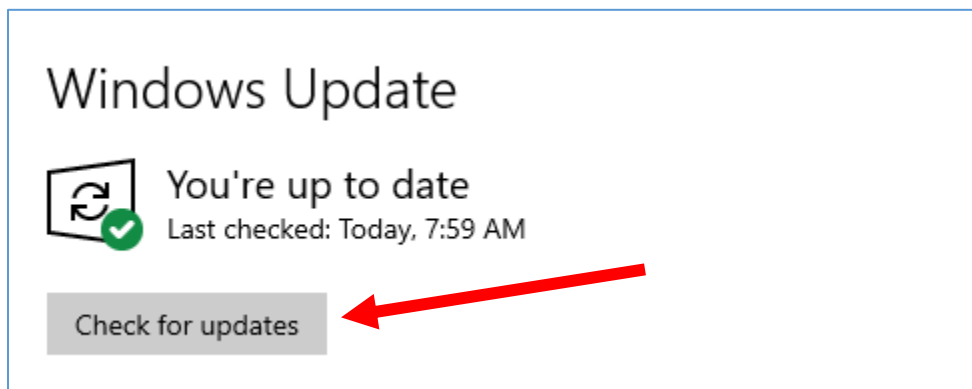
شکل ۲- Crash کردن سیستم آسیب‌پذیر

۴- نحوه مقابله

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

۴-۱- روش اول – به‌روزرسانی خودکار (توصیه می‌شود)

سیستم خود را به اینترنت متصل کنید و در منوی استارت ویندوز update را تایپ کنید و روی windows update و در صفحه باز شده Check for updates (شکل ۳) کلیک کنید و مدت طولانی منتظر بمانید تا ویندوز شما آپدیت شود و در نهایت سیستم را Restart کنید.



شکل ۳- شروع بروزرسانی ویندوز

۴-۲- روش دوم - به روزرسانی دستی

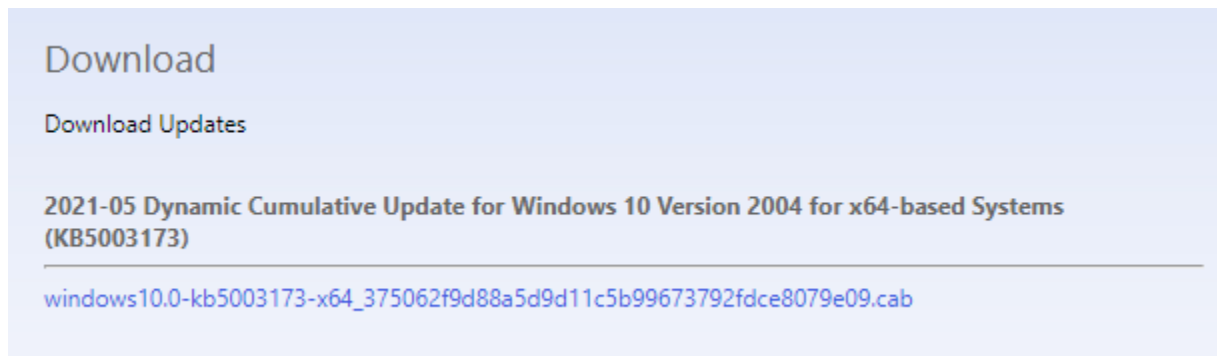
اگر به هر دلیلی امکان به‌روزرسانی خودکار برای شما وجود ندارد از این روش استفاده کنید. ابتدا با نوشتن winver در run یا منو استارت ویندوز نسخه دقیق ویندوز را تعیین کنید. پس از تعیین نسخه دقیق ویندوز به [صفحه توضیحات آسیب‌پذیری بروید](#)^۳ و در بخش Security Updates متناسب با نسخه ویندوز خود آپدیت مناسب را انتخاب کنید و با کلیک روی Security Update به صفحه دانلود به‌روزرسانی بروید. در صفحه دانلود بازهم متناسب با نسخه ویندوز خود روی دکمه Download کلیک کنید (شکل ۴).

Title	Products	Classification	Last Updated	Version	Size	Download
2021-05 Cumulative Update for Windows Server, version 2004 for x64-based Systems (KB5003173)	Windows Server, version 1903 and later	Security Updates	5/10/2021	n/a	572.6 MB	Download
2021-05 Cumulative Update for Windows 10 Version 2004 for x64-based Systems (KB5003173)	Windows 10, version 1903 and later	Security Updates	5/10/2021	n/a	572.6 MB	Download
2021-05 Cumulative Update for Windows 10 Version 2004 for x86-based Systems (KB5003173)	Windows 10, version 1903 and later	Security Updates	5/10/2021	n/a	270.4 MB	Download
2021-05 Cumulative Update for Windows Server, version 2004 for ARM64-based Systems (KB5003173)	Windows Server, version 1903 and later	Security Updates	5/10/2021	n/a	619.3 MB	Download
2021-05 Cumulative Update for Windows 10 Version 2004 for ARM64-based Systems (KB5003173)	Windows 10, version 1903 and later	Security Updates	5/10/2021	n/a	619.3 MB	Download
2021-05 Cumulative Update for Windows Server, version 20H2 for x64-based Systems (KB5003173)	Windows Server, version 1903 and later	Security Updates	5/10/2021	n/a	572.6 MB	Download
2021-05 Cumulative Update for Windows 10 Version 20H2 for x64-based Systems (KB5003173)	Windows 10, version 1903 and later	Security Updates	5/10/2021	n/a	572.6 MB	Download
2021-05 Cumulative Update for Windows 10 Version 20H2 for x86-based Systems (KB5003173)	Windows 10, version 1903 and later	Security Updates	5/10/2021	n/a	270.4 MB	Download
2021-05 Cumulative Update for Windows Server, version 20H2 for ARM64-based Systems (KB5003173)	Windows Server, version 1903 and later	Security Updates	5/10/2021	n/a	619.3 MB	Download
2021-05 Cumulative Update for Windows 10 Version 20H2 for ARM64-based Systems (KB5003173)	Windows 10, version 1903 and later	Security Updates	5/10/2021	n/a	619.3 MB	Download
2021-05 Dynamic Cumulative Update for Windows 10 Version 2004 for x64-based Systems (KB5003173)	Windows 10 GDR-DU	Security Updates	5/10/2021	n/a	571.5 MB	Download
2021-05 Dynamic Cumulative Update for Windows 10 Version 2004 for x86-based Systems (KB5003173)	Windows 10 GDR-DU	Security Updates	5/10/2021	n/a	269.8 MB	Download
2021-05 Dynamic Cumulative Update for Windows 10 Version 2004 for ARM64-based Systems (KB5003173)	Windows 10 GDR-DU	Security Updates	5/10/2021	n/a	618.3 MB	Download
2021-05 Dynamic Cumulative Update for Windows 10 Version 20H2 for x64-based Systems (KB5003173)	Windows 10 GDR-DU	Security Updates	5/10/2021	n/a	571.5 MB	Download
2021-05 Dynamic Cumulative Update for Windows 10 Version 20H2 for x86-based Systems (KB5003173)	Windows 10 GDR-DU	Security Updates	5/10/2021	n/a	269.8 MB	Download
2021-05 Dynamic Cumulative Update for Windows 10 Version 20H2 for ARM64-based Systems (KB5003173)	Windows 10 GDR-DU	Security Updates	5/10/2021	n/a	618.3 MB	Download

شکل ۴- صفحه دانلود آپدیت

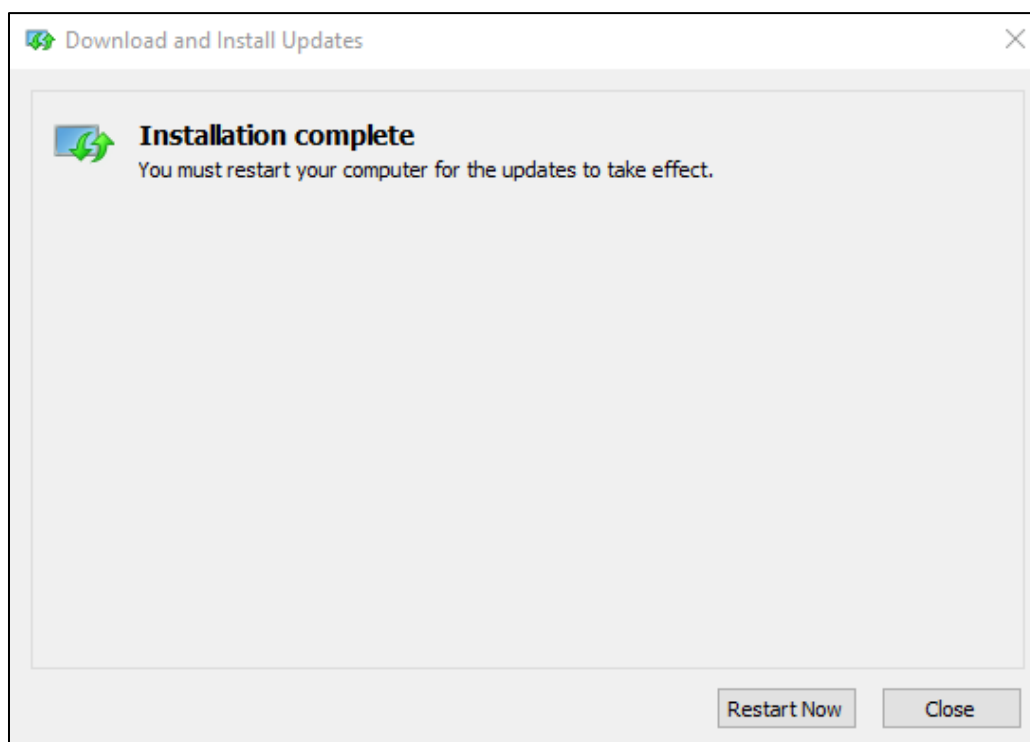
در صفحه باز شده روی لینک آپدیت مورد نظر (شکل ۵) کلیک کنید تا دانلود فایل آغاز شود.

^۳ <https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-31166>



شکل ۵- لینک دانلود آپدیت

پس از دانلود، فایل دریافتی که با نامی مشابه windows10.0-kbxxx-xxxxxxxxxxxxx.msu است را اجرا کنید و روی Yes کلیک کنید تا نصب آپدیت آغاز شود. در پایان پیام شکل ۶ نمایش داده می‌شود و روی Restart Now کلیک کنید تا نصب تکمیل شود.



شکل ۶- پایان نصب آپدیت

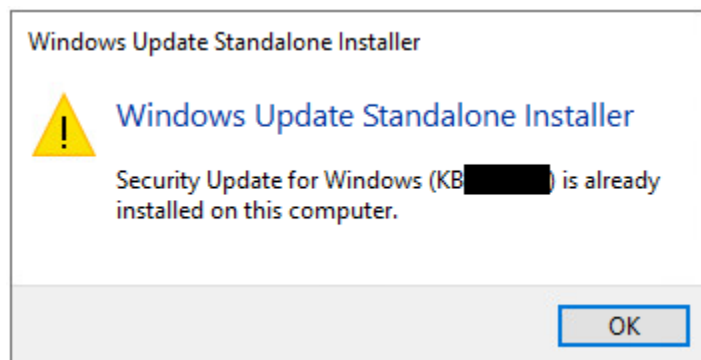
۵- بررسی نصب‌بودن به‌روزرسانی

به‌روزرسانی برای CVE-2021-31166 برای تمامی نسخه‌های آسیب‌پذیر ویندوز با نام KB5003173 منتشر شده است. با روش‌های زیر از نصب این به‌روزرسانی اطمینان حاصل کنید.



۵-۱- روش اول

فایل نصب آپدیت را دوباره اجرا کنید اگر نصب باشد به شما پیام شکل ۷ نمایش داده می‌شود (شکل ۶).



شکل ۷- پیام نصب بودن آپدیت

۵-۲- روش دوم

برای بررسی نصب‌بودن به‌روزرسانی روی یک سیستم، update history را در منو استارت ویندوز تایپ کنید و در برگه View update history به دنبال نام به‌روزرسانی آن (KB5003173) بگردید (شکل ۸).

View update history

[Uninstall updates](#)

[Recovery options](#)

Update history

Quality Updates (7)

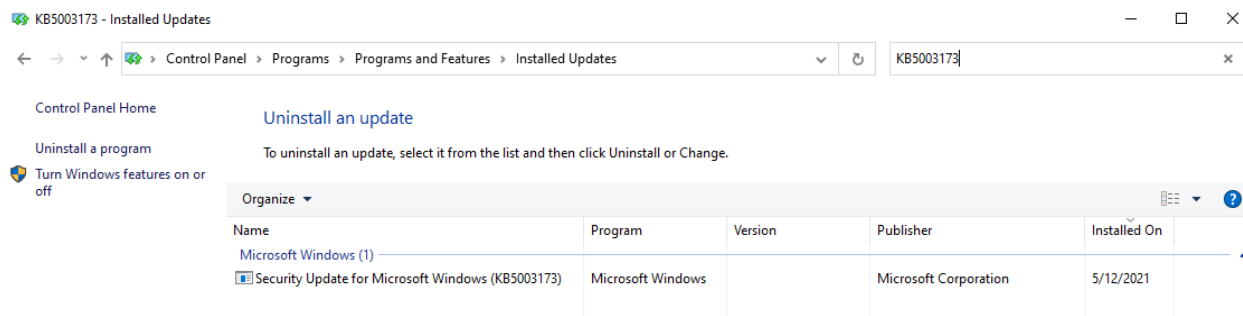
2021-05 Cumulative Update for Windows 10 Version 2004 for x64-based Systems (KB5003173)

Successfully installed on 5/15/2021

شکل ۸- بررسی نصب آپدیت

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 ۹).



شکل ۹- بررسی نصب آپدیت روش دوم

۴-۵- روش چهارم (حرفه‌ای)

در powershell دستور `Get-HotFix -Id KB5003173` با نام به‌روزرسانی KB5003173 را وارد کنید اگر آپدیت نصب شده باشد خروجی باید به شکل ۱۰ باشد وگرنه پیام خطا نمایش داده می‌شود.

```
PS C:\Users\ [redacted] > Get-HotFix -Id KB5003173
```

Source	Description	HotFixID	InstalledBy	InstalledOn
[redacted]	Security Update	KB5003173	[redacted]	5/12/2021 12:00:00 AM

شکل ۱۰- بررسی نصب با PowerShell

تا آسیب‌پذیری جدید بدرود! ☺

درباره ما:

گروه امنیت سایبری امن بان 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 امن بان فناوری‌های پیشرفته شریف با شماره ثبت ۵۴۴۸۹۴ و اخذ مجوز از مراجع ذی صلاح با نام تجاری امن بان ادامه یافت. همچنین مجموعه امن بان 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

