گزارش آسیب‌پذیری PrintNightmare

شرح آسیب‌پذیری CVE-2021-34527 و نحوه رفع آن

شماره گزارش VU00702

مرداد ۱۴۰۰

گروه امنیت سایبری امن‌بان
AMN BAN
CYBER SECURITY GROUP

تهران، آزادراه تهران ـ کرج، بلوار چوگان، روبروی شهرک آزادی، پردیس نوآوری شهید مقدم، واحد ۵

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

۵- حق چاپ و نشر

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

رفع مسئولیت

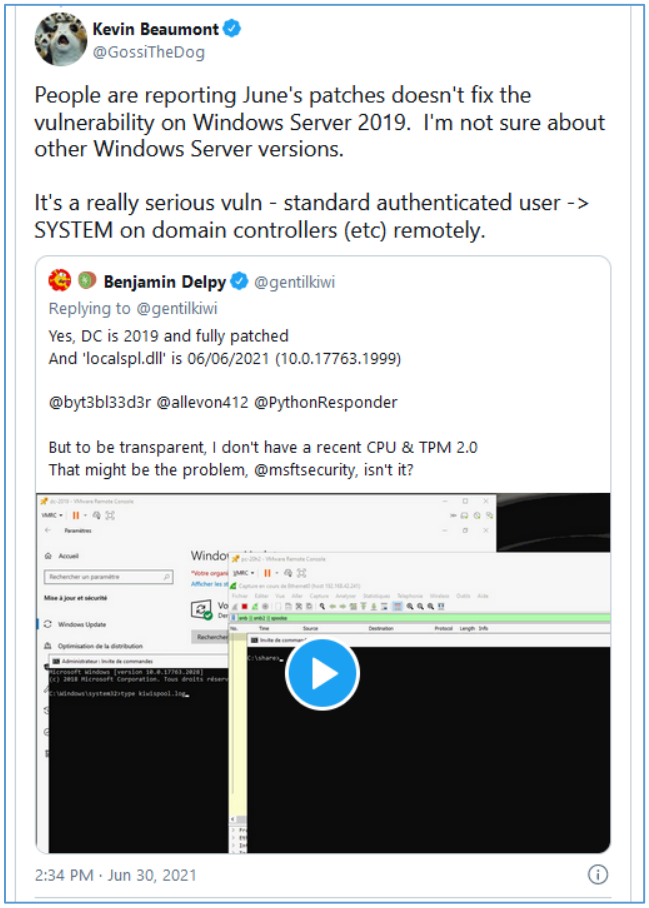
شرکت «امن‌بان فناوری‌شریف» هیچگونه مسئولیتی در قبال سوء استفاده یا مشکلات استفاده از این گزارش ندارد و کلیه مسئولیت بر عهده استفاده کننده می‌باشد.

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

بعد از آسیب‌پذیری با شناسه CVE-2021-1675 روی سرویس print spooler که منجر به اجرای دستور از راه دور (RCE) می‌شد یک بهره‌جویی[۱] توسط Benjamin Delpy خالق ابزار معروف mimikatz روی ویندوز سرور ۲۰۱۹ که تا تاریخ 2021/06/06 هم آپدیت شده بود منتشر شد[۲] (شکل ۱)، در ابتدا تصور می‌شد که آپدیت مایکروسافت برای این آسیب‌پذیری درست عمل نکرده اما بعداً معلوم شد که یک آسیب‌پذیری جدید است و با شناسه CVE-2021-34527 و نام PrintNightmare نامگذاری شد. این آسیب‌پذیری نیز منجر به اجرای کد ازراه‌دور (RCE) روی سیستم قربانی می‌شد. چند روز پس از انتشار آسیب‌پذیری CVE-2021-34527 یک وصله‌ی[۳] اولیه برای رفع آن توسط شرکت مایکروسافت منتشر شد که بهره‌جویی هم آپدیت شد و نشان داد که آپدیت منتشرشده مشکل را کامل رفع نکرده است و در نهایت مایکروسافت آپدیت کاملی برای این آسیب پذیری ارائه داد.



شکل ۱- عمل‌کردن بهره‌جویی روی ویندوز سرور ۲۰۱۹ به روز

---

۱ Exploit

۲ https://github.com/gentilkiwi/mimikatz/releases/tag/2.2.0-20210701

۳ Patch

آسیب‌پذیری CVE-2021-34527 دارای امتیاز CVSS 8.8 است اما به علت وجود آسیب‌پذیری روی سرویس Print Spooler (به صورت پیش‌فرض روی Domain Controllerها توسط سیستم‌های عضو دامنه قابل دسترس است) و امکان دسترسی راحت به آن اهمیت بالایی پیدا کرده است.

بهره‌جویی این آسیب‌پذیری از راه دور توسط یک سیستم عضو دامنه قابل انجام است و نیاز به احراز هویت و تعامل کاربر ندارد. مهاجم به کمک این آسیب‌پذیری می‌تواند به‌صورت راه‌دور کد دلخواه موردنظر خود را اجرا کند.

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

۲- آسیب‌پذیری CVE-2021-34527 چه آثار مخربی دارد؟

از آنجا که با بهره‌جویی از این آسیب‌پذیری امکان اجرای کد از راه‌دور وجود دارد، مهاجم می‌تواند کد دلخواه خود را روی سرور مهم Domain Controller اجرا کند. بنابراین این آسیب‌پذیری بسیار مهم می‌باشد.

۳- چه سیستم‌هایی تحت تاثیر این آسیب پذیری قرار دارند؟

طبق اعلام مایکروسافت[۴] این آسیب‌پذیری روی ویندوز سرور 2004, 2008, 2008R2, 2012, 2012R2, 2016, 2019, 20H2 و ویندوزهای 7, 8.1, RT8.1, 10 وجود دارد.

برای بررسی آسیب‌پذیربودن یک سیستم، هنوز اسکریپت یا ابزار غیر مخرب و معتبری منتشر نشده است که محض انتشار اطلاع‌رسانی خواهد شد. البته از ابزارهایی مانند mimikatz می‌توان استفاده کرد که چون ممکن است باعث خرابی DC شود اینکار توصیه نمی‌شود.

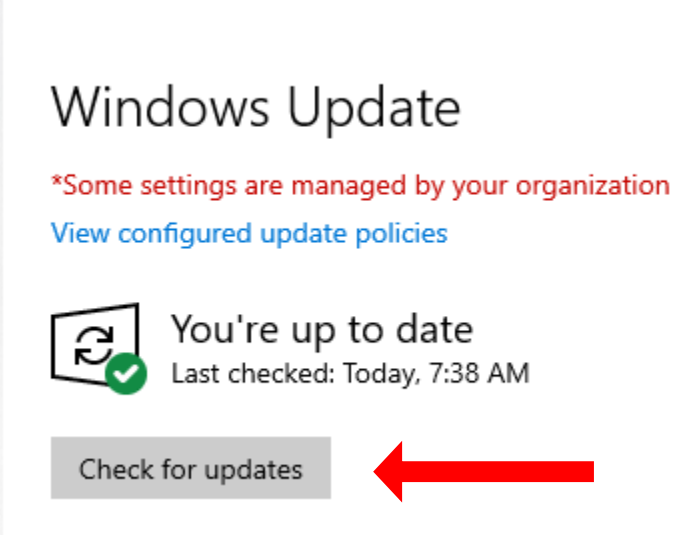
۴- نحوه مقابله

برای رفع این آسیب‌پذیری می‌توانید به‌روزرسانی مربوطه را طبق دستورالعمل‌های زیر نصب کنید و یا سرویس spooler را غیرفعال کنید. البته توجه داشته باشید که غیرفعال کردن این سرویس روی سیستم‌هایی که پرینتر اشتراکی دارند مشکلاتی ایجاد خواهد کرد.

۴-۱- نصب به‌روزرسانی به‌صورت 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 بازشده Check for updates (شکل ۲) کلیک کنید و مدت طولانی منتظر بمانید تا ویندوز شما آپدیت شود و درنهایت سیستم را Restart کنید.

[۴] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-1675

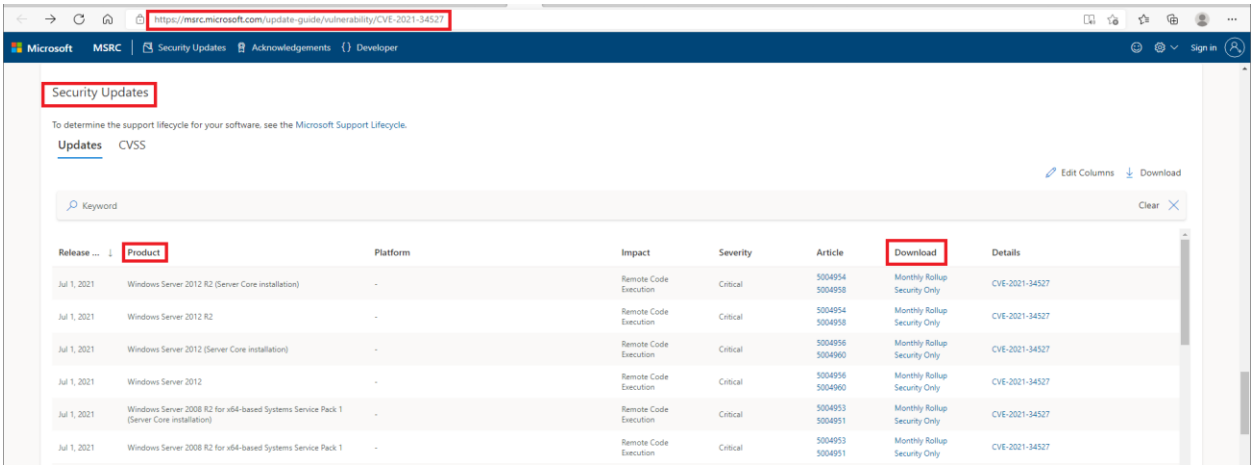


شکل ۲- شروع به‌روزرسانی ویندوز

۲-۴- نصب به‌روزرسانی به‌صورت 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[۵] و در بخش Security Updates متناسب با نسخه ویندوز خود آپدیت مناسب را انتخاب کنید و نصب کنید (شکل ۳).



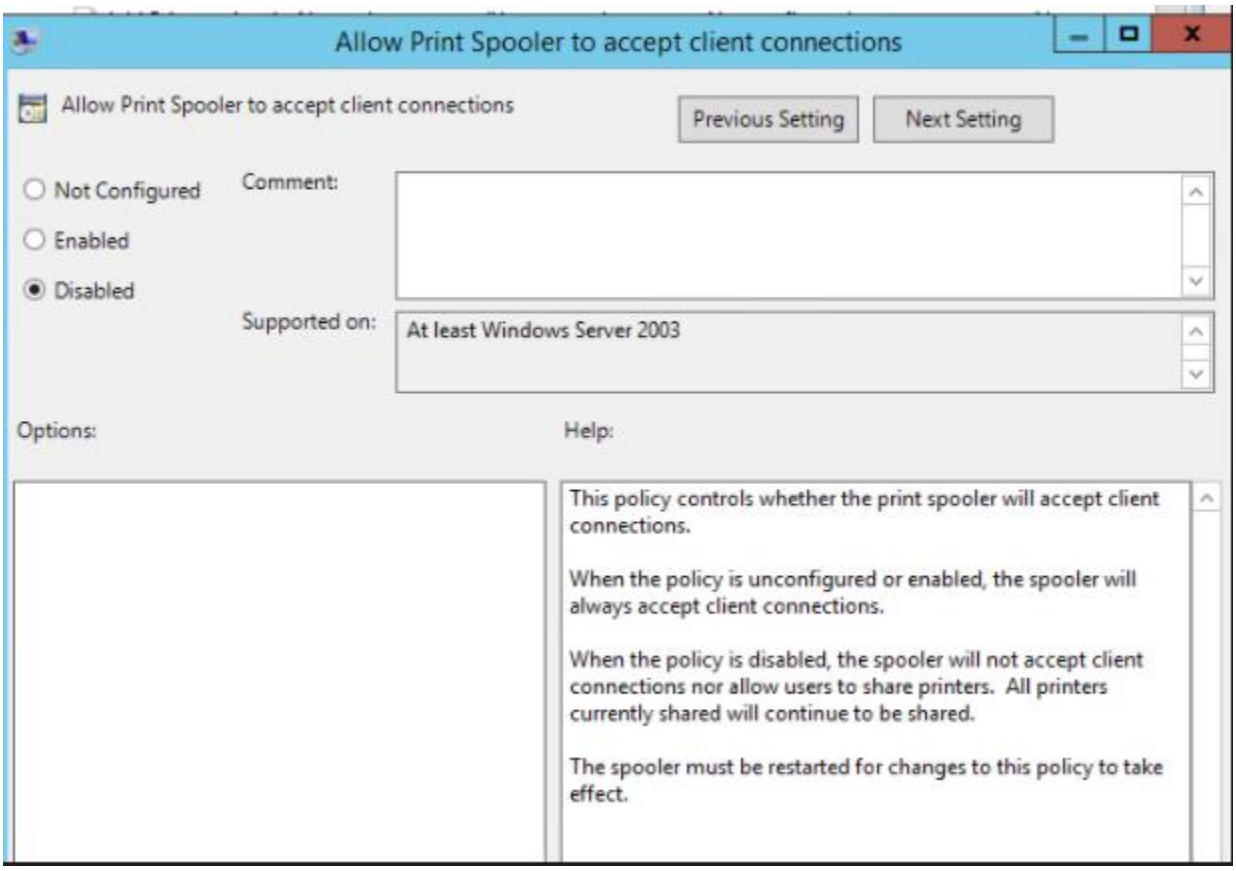
شکل ۳ – صفحه انتخاب به‌روزرسانی بر اساس نسخه سیستم‌عامل

[۵] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

۳-۴- غیرفعال‌کردن سرویس spooler

برای مقابله با این آسیب‌پذیری می‌توانید سرویس spooler را از طریق GPO غیرفعال کنید. تنظیمات سرویس spooler در مسیر زیر قرار دارد و باید مانند شکل ۴ روی Disabled قرار گیرد.

Computer Configuration -> Administrative Templates -> Printers -> Allow Print Spooler to accept client connections



شکل ۴- غیرفعال‌سازی سرویس **Spooler**

در صورتی که روی سرورها و سیستم های خود به سرویس Print Spooler یا سرویس‌های مشابه نیاز ندارید آنها را غیرفعال کنید یا حداقل از دسترسی به آنها از طریق شبکه به کمک Firewall ویندوز جلوگیری کنید.

تا آسیب‌پذیری جدید بدرود! ☺

درباره ما:

گروه امنیت سایبری امن‌بان به همت جمعی از فارغ التحصیلان دانشگاه صنعتی شریف و امیرکبیر 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 و اخذ مجوز از مراجع ذی صلاح با نام تجاری امن‌بان ادامه یافت.

امن‌بان در حوزه تست نفوذ شبکه و وب سایت، Red Teaming، امن سازی سرورها و سامانه‌ها، ارزیابی امنیتی محصولات و تحلیل بدافزار و باج افزار فعالیت می‌کند.

امن‌بان دارای مجوز تست نفوذ و آموزش افتا از سازمان فناوری اطلاعات و مرکز مدیریت راهبردی افتا است، همچنین 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