بسمه‌تعالی

وزارت ارتباطات و فناوری اطلاعات

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر

مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه ای

هشدار: آسیب‌پذیری در سرویس Print Spooler ویندوز

خبر به‌روزرسانی

شناسه سند	MaherReports_14000410-01
نوع سند	گزارش فنی
شماره نگارش	۰,۱
تاریخ نگارش	۱۴۰۰/۰۴/۱۰
طبقه‌بندی سند	عادی

تهران، خیابان شهید بهشتی- بین بزرگراه شهید مدرس و خیابان احمد قصیر- پلاک ۲۶۷

(۰۲۱) ۴۲۶۵۰۰۰۰ (۰۲۱) ۴۲۶۵۰۰۰۰ cert.ir

فهرست مطالب

اخیراً آسیب‌پذیری جدیدی با شناسه‌ی CVE-2021-1675 و شدت بالا (۷,۸ از ۱۰) در سرویس Print Spooler ویندوز کشف شده است که بهره‌برداری از آن منجر به اجرای کد از راه دور بر روی سیستم ویندوزی و در اختیار گرفتن آن توسط مهاجم خواهد شد؛ لازم به ذکر است که مهاجم برای بهره‌برداری به امتیاز یا دسترسی بالایی نیاز ندارد. با توجه داشت که سرویس Print Spooler به صورت پیش‌فرض در سیستم‌های ویندوزی در حال اجرا است و برای اجرا نیاز به اتصال به یک دستگاه پرینتر ندارد.

به لحاظ فنی این آسیب‌پذیری که با نام **PrintNightmare** شناخته می‌شود، ناشی از محدود نکردن دسترسی به تابع RpcAddPrinterDriverEx() است که برای یک مهاجم احراز هویت شده (standard user account)، امکان اجرای کد از راه دور با دسترسی SYSTEM بر روی سیستم آسیب‌پذیر را فراهم می‌کند.

۱ محصولات آسیب‌پذیر

با توجه به اینکه مایکروسافت از این آسیب‌پذیری به عنوان یک آسیب‌پذیری **بحرانی** یاد کرده است و کد اکسپلویت این آسیب‌پذیری در سطح اینترنت منتشر شده و در دسترس عموم قرار گرفته است، هرچه سریع‌تر نسبت به به‌روزرسانی محصولات آسیب‌پذیر اقدام کنید. **درصورتی‌که از ویندوز سرور به عنوان کنترل کننده‌ی دامنه (DC) استفاده می‌کنید ممکن است اعمال وصله‌های امنیتی در رفع آسیب‌پذیری موثر نباشد.**

جدول ۱: فهرست محصولات آسیب‌پذیر

نام محصول	نوع آسیب‌پذیری	شدت آسیب‌پذیری از ۱۰	شناسه آسیب‌پذیری
Windows Server 2012 R2 Windows Server 2012 Windows Server 2008 R2 Windows Server 2008 Windows Server 2016 Windows Server, version 20H2 Windows Server, version 2004 Windows Server 2019	اجرای کد از راه دور	۷,۸	CVE-2021-1675 (**PrintNightmare**)
Windows 8.1 Windows 7 Windows 10			

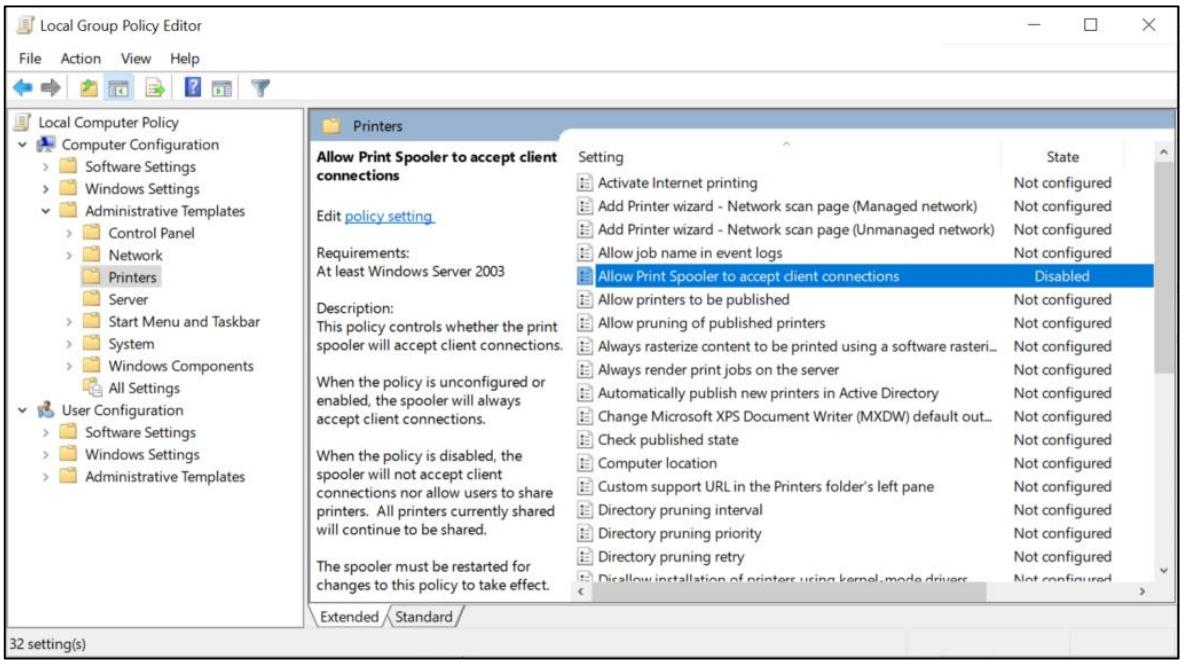
۲ عدم رفع آسیب‌پذیری در برخی سیستم‌های وصله شده

در برخی موارد مشاهده شده است که ویندوز سرورهایی که به عنوان کنترل‌کننده دامنه (DC) فعالیت می‌کنند پس از دریافت وصله همچنان آسیب‌پذیر بوده و امکان اجرای کد از راه دور بر روی آنها وجود دارد؛ به عنوان مثال اگر مقدار فیلد «NoWarningNoElevationOnInstall» در تنظیمات group policy، «یک» تنظیم شده باشد، سیستم DC پس از دریافت وصله همچنان آسیب‌پذیر خواهد بود. برای مشاهده‌ی مقدار فیلد مذکور به آدرس زیر در DC مراجعه کنید:

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Printers\PointAndPrint**NoWarningNoElevationOnInstall**

با توجه به اینکه یکی از کدهای اکسپلویت منتشر شده به طور خاص کنترل‌کننده‌های دامنه (DC) Active Directory را هدف قرار داده است و برخی سیستم‌های DC پس از به‌روزرسانی آسیب‌پذیر باقی می‌مانند، **اکیداً** توصیه می‌گردد سرویس Print spooler ویندوز را در کنترل‌کننده‌های دامنه و سیستم‌های که از خدمت پرینت استفاده نمی‌کنند (با تغییر Group Policy)، **غیرفعال کنید** تا در صورت هدف قرار گرفتن توسط مهاجمان، کل شبکه داخلی سازمان تحت اختیار مهاجمان قرار نگیرد. توجه داشته باشید که سرویس باید غیرفعال شود (disabled) نه متوقف (Stopped)؛ چراکه در صورت متوقف کردن سرویس، مهاجم می‌تواند مجدداً آن را راه‌اندازی کند.

از آنجایی که عموماً کلاینت‌ها نیاز به استفاده از این سرویس دارند به جای غیرفعال کردن سرویس می‌توان پیکربندی آن را طوری تغییر داد که امکان برقراری اتصال از سایر کلاینت از بین برود. به این منظور به صورت محلی یا با استفاده از تنظیمات Group Policy مطابق شکل ۱ « Allow Print Spooler to accept client connections» را بر روی Disabled تنظیم کنید.



شکل ۱

غیرفعال کردن سرویس Print spooler در رابط‌های Command line و PowerShell:

```
Command line: net stop spooler && sc config spooler start=disabled

PowerShell: Stop-Service -Name Spooler -Force Set-Service -Name Spooler -StartupType Disabled
```

لازم به ذکر است که آسیب‌پذیری‌های موجود در سرویس Print Spooler پیش‌تر نیز توسط بدافزارها و ویروس‌های کامپیوتری مورد بهره‌برداری قرار گرفته‌اند (CVE-2010-2729).

۳ مراجع

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

[۲] https://docs.microsoft.com/en-us/defender-for-identity/cas-isp-print-spooler

[۳] https://doublepulsar.com/zero-day-for-every-supported-windows-os-version-in-the-wild-printnightmare-b3fdb82f840c

[۴] https://blog.truesec.com/2021/06/30/exploitable-critical-rce-vulnerability-allows-regular-users-to-fully-compromise-active-directory-printnightmare-cve-2021-1675/