BOLETÍN DE ALERTA

Boletín Nro.: 2021-15

Fecha de publicación: 02/07/2021

Tema: Vulnerabilidad 0-day de RCE en el servicio Print Spooler de Microsoft Windows.

Fecha de actualización: 11/07/2021

Sistemas afectados:

- Windows Server 2016;
- Windows Server 2019;
- Windows Server 2012 (incluyendo R2);
- Windows Server 2008 (incluyendo R2, R2 SP1 y R2 SP2);
- Windows 7, 8.1 y 10 (incluyendo versión 1909);
- Windows Server, versiones 2004 y 20H2.

Descripción:

La vulnerabilidad CVE-2021-1675, también conocida como "PrintNightmare" se calificó inicialmente como una vulnerabilidad de elevación de privilegios de baja importancia y fue parcheada en el pasado Martes de Parches de Microsoft de junio de 2021. Semanas después Microsoft cambió la clasificación de la vulnerabilidad porque se descubrió que la falla permite la ejecución remota de código (RCE) y se re-clasificó como crítica debido a que investigadores de la firma de seguridad china QiAnXin publicaron un GIF en Twitter que mostraba un exploit funcional para la falla CVE-2021-1675, pero evitaron revelar los detalles técnicos sobre el ataque.

Para evitar confusiones, Microsoft ha asignado a esta vulnerabilidad RCE un nuevo identificador CVE, CVE-2021-34527 de severidad alta con una puntuación de 8.8. La vulnerabilidad afecta al servicio Print Spooler, que está habilitado de forma predeterminada en los sistemas Windows, y permite a los atacantes engañar a este servicio para que instalen un controlador de impresión alojado de forma remota utilizando una cuenta de usuario con pocos privilegios. La explotación exitosa permite que los atacantes ejecuten

código en el sistema de destino (Ejecución Remota de Código - RCE) en el contexto del servicio de cola de impresión que se ejecuta con privilegios de SISTEMA (escalamiento de privilegios).

Los Controladores de Dominio (Active Directory) están particularmente expuestos, ya que un atacante, que ha comprometido previamente la estación de trabajo de un usuario, puede finalmente obtener los derechos y privilegios en el nivel de "administrador de dominio".

Para lograr la ejecución remota de código (RCE), el atacante debería apuntar a un usuario autenticado en el servicio de cola de impresión. Sin autenticación, la falla podría aprovecharse para elevar los privilegios, haciendo de esta vulnerabilidad un vínculo valioso en una cadena de ataque.

Windows Print Spooler

Print Spooler es una aplicación/interfaz/servicio que interactúa con impresoras locales o en red y administra el proceso de impresión.

Prueba de concepto PoC

Durante junio, investigadores de la empresa china de ciberseguridad QiAnXin compartieron en Twitter un video/GIF que mostraba un exploit de la vulnerabilidad para lograr RCE.

Unos días después, los investigadores de Sangfor Technologies publicaron y luego eliminaron rápidamente detalles técnicos y el exploit de la PoC para la CVE-2021-1675, pero se estima que el repositorio donde lo colocaron fue clonado/bifurcado, lo que ha permitido la aparición en GitHub de repositorios con PoC funcional haciendo la siguiente mención: *“PoC creado originalmente por Zhiniang Peng (@edwardzpeng) y Xuefeng Li (@ lxf02942370)”*

Impacto:

La explotación exitosa de la vulnerabilidad podría dar a los atacantes remotos el control total de los sistemas vulnerables.

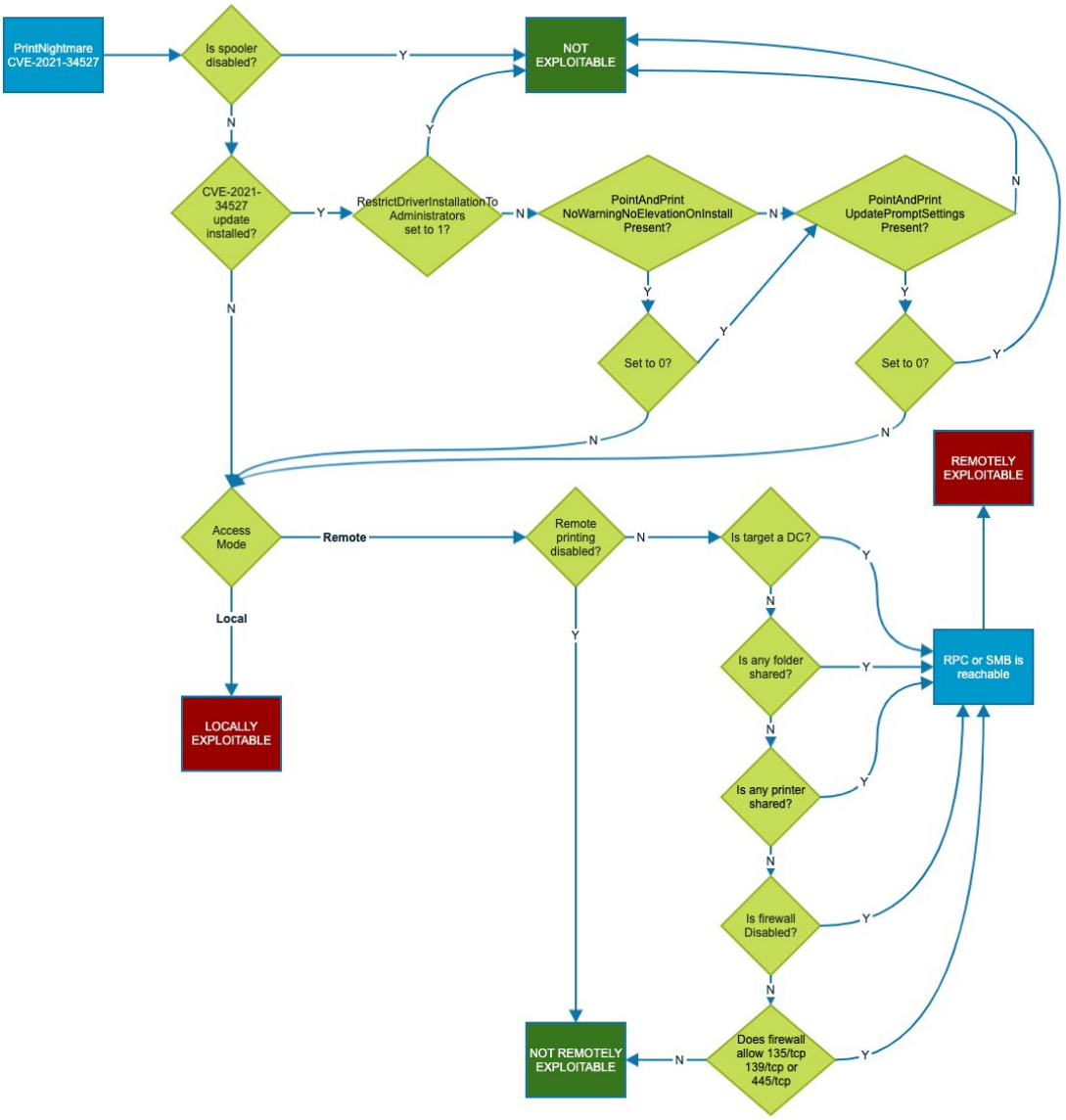
Solución:

Microsoft ha publicado actualizaciones de seguridad para abordar esta vulnerabilidad. Consulte la Tabla de Actualizaciones de Seguridad para conocer la actualización correspondiente a su sistema. Le recomendamos que instale estas actualizaciones de inmediato.

La actualización por sí sola no soluciona la vulnerabilidad si se tienen ciertos registros activos y/o definidos:

- HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint
- NoWarningNoElevationOnInstall = 0 (DWORD) o no definido (configuración por defecto)
- UpdatePromptSettings = 0 (DWORD) o no definido (configuración por defecto)
- **Tener NoWarningNoElevationOnInstall configurado a 1 hace que el sistema sea vulnerable de diseño.**

La situación es descrita en la Tabla de Actualizaciones de Seguridad de Microsoft . A continuación adjuntamos una imagen que aclara la situación de mejor manera los casos en qué casos se soluciona la vulnerabilidad y en qué casos no.



Esta imagen fue creada por un investigador de confianza miembro del equipo CERT/CC https://twitter.com/wdormann/status/1413210835326054402/photo/1.

Si desea más detalles sobre la misma puede consultar la nota publicada por el equipo CERT/CC https://www.kb.cert.org/vuls/id/383432.

Si no puede instalar estas actualizaciones o aún Microsoft no provee el parche para su sistema, siga las instrucciones de mitigación.

Mitigación:

- **Deshabilitar el Print Spooler**

  Determinar si el servicio de cola de impresión se está ejecutando:

```
Get-Service -Name Spooler
```

  Si la cola de impresión se está ejecutando o si el servicio no está deshabilitado, seleccione una de las siguientes opciones para deshabilitar el servicio de cola de impresión o para deshabilitar la impresión remota entrante a través de la directiva de grupo:

  Opción 1: deshabilitar el servicio de cola de impresión (desactiva la capacidad de imprimir tanto de forma local como remota)

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

  Opción 2: deshabilitar la impresión remota entrante a través de la directiva de Grupo (el sistema ya no funcionará como servidor de impresión remoto). Se debe configurar los ajustes a través de la Política de Grupo de la siguiente manera:

  - ☐ **Configuración de la computadora / Plantillas administrativas / Impresoras**
  - ☐ Deshabilite la política **"Permitir que la cola de impresión acepte conexiones de cliente:"** para bloquear ataques remotos.
  - ☐ Debe reiniciar el servicio de cola de impresión para que la política de grupo surta efecto.

- ☐ Para obtener más información, consulte: Usar la configuración de la directiva de grupo para controlar las impresoras.

- **Para ambientes de prueba y/o desarrollo:** Se ha proporcionado una nueva estrategia de defensa, que consiste en restringir las listas de control de accesos (ACLs), para hacer que el exploit no sea efectivo, mientras que se permite mantener sus servidores de impresión en funcionamiento, hasta que un parche esté disponible.

Detección:

- Módulo CrackMapExec para detectar si el servicio de cola de impresión está habilitado o no de forma remota.

  Instalación:

  1. Docker:

```
docker pull byt3bl33d3r/crackmapexec
```

  2. Paquete Python

```
#~ python3 -m pip install pipx
#~ pipx ensurepath
#~ pipx install crackmapexec
```

  3. Desde la fuente

```
#~ apt-get install -y libssl-dev libffi-dev python-dev build-essential
#~ git clone --recursive https://github.com/byt3bl33d3r/CrackMapExec
#~ cd CrackMapExec
#~ poetry install
#~ poetry run crackmapexec
```

- Escáner Python ItWasAllADream para CVE-2021-34527, permite escanear subredes enteras para PrintNightmare RCE (no LPE) y generar un informe CSV con los resultados.

Instalación:

1. Docker:

```
git clone https://github.com/byt3bl33d3r/ItWasAllADream
cd ItWasAllADream && docker build -t itwasalladream .
docker run -it itwasalladream -u user -p password -d domain
192.168.1.0/24
```

2. Instalación en modo desarrollador requiere Poetry:

```
git clone https://github.com/byt3bl33d3r/ItWasAllADream
cd ItWasAllADream && poetry install && poetry shell
itwasalladream -u user -p password -d domain 192.168.1.0/24
```

Como el exploit requiere que esté autenticado en Active Directory, debe proporcionar credenciales. Si no se proporciona la contraseña, se le pedirá que la ingrese.

Información adicional:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1675
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527
- https://github.com/byt3bl33d3r/CrackMapExec
- https://github.com/byt3bl33d3r/ItWasAllADream
- https://es-la.tenable.com/blog/cve-2021-1675-proof-of-concept-leaked-for-critical-windows-print-spooler-vulnerability?tns_redirect=true
- https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/vulnerabilidad-0day-rce-el-servicio-print-spooler-microsoft-windows