BOLETÍN DE ALERTA

Boletín Número: 2021-06. **Fecha de Publicación:** 12/07/2021

Tema: Nueva actualización vulnerabilidad Microsoft

Importancia: Crítica.

Descripción:

El Departamento de Ciberseguridad de la DIGETIC/FFAA, informa de la publicación de nuevas actualizaciones en la vulnerabilidad CVE-2021-34527 que afecta a los sistemas operativos de Microsoft.

Tras la publicación por parte de Microsoft del parche de seguridad para solventar la vulnerabilidad conocida como PrintNightmare, a la que se le asignó el CVE-2021-34527 y que afecta al servicio Windows Print Spooler permitiendo ejecutar código de forma remota (RCE) y escalar privilegios dentro del sistema, varios investigadores han descubierto que se impide la ejecución de código remota pero no la escalada de privilegios a nivel local. Además si la directiva 'Restricciones de apuntar e imprimir' está habilitada permite seguir ejecutando código de forma remota.

Recursos Afectados:

- Todas las versiones de los sistemas operativos Windows

Solución:

Una vez aplicado el parche publicado por Microsoft, se debe comprobar que la siguiente configuración del Registro de Windows está establecida en cero o no está definida:

- 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).

Si alguna de las condiciones no es cierta, el sistema es vulnerable, por lo tanto, se debe configurar la política de grupo de restricciones de impresión de la siguiente manera:

- Abrir la herramienta de edición de políticas de grupo:
- Configuración del equipo >Plantillas administrativas > Impresoras.
- Establecer la configuración de la política de grupo de restricciones de impresión (Point and Point Restrictions) de la siguiente manera:
- Chequear opción "Habilitada".
- Al instalar controladores para una nueva conexión: "Mostrar advertencia y aviso de elevación".

- Al actualizar los controladores para una conexión existente: "Mostrar advertencia y aviso de elevación".

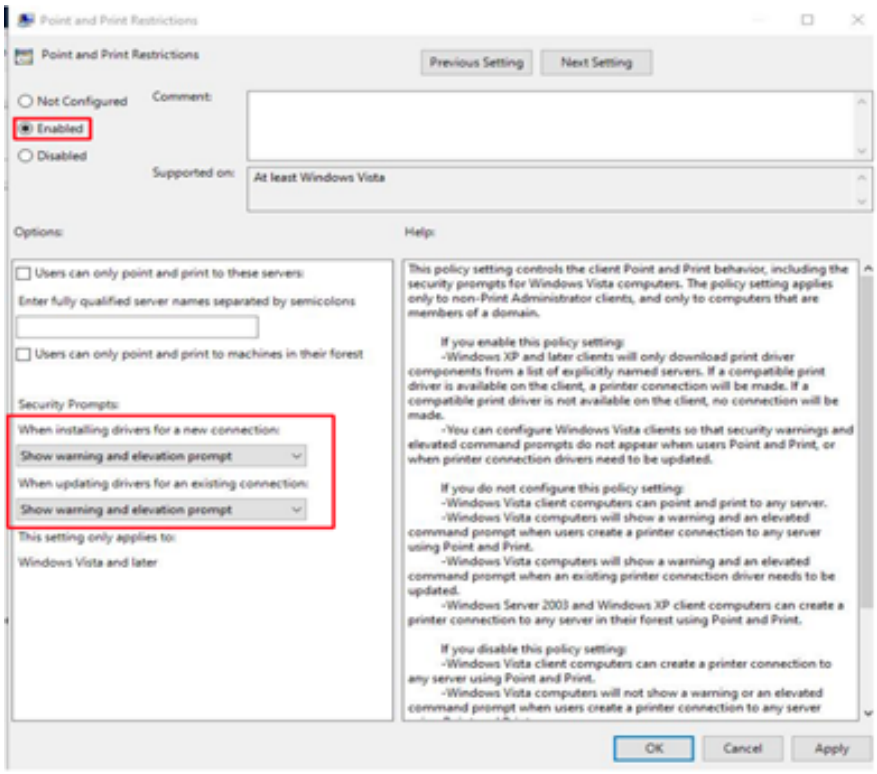

Imagen: solución alternativa Microsoft.

Además, se indica una medida opcional que implica anular las restricciones de punto de impresión y forzar la instalación del controlador sólo a los administradores (estableciendo con el valor 1 el parámetro vRestrictDriverInstallation). Establecer este valor en 1 o cualquier valor distinto de cero evita que un usuario que no sea administrador instale cualquier controlador de impresora. Para automatizar la adición del valor de registro:

- Abrir una ventana del símbolo del sistema (cmd.exe) con permisos de root.
- Escribir el siguiente comando:
    - reg add "HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsNT\Printers\PointAndPrint"/vRestrictDriverInstallationToAdministrators/t REG_DWORD/d1/f

Referencias:

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34527
https://support.microsoft.com/es-es/topic/kb5005010-restricting-installation-of-new-printer-drivers-after-applying-the-july-6-2021-updates-31b91c02-05bc-4ada-a7ea-183b129578a7
https://www.genbeta.com/actualidad/fallido-parche-seguridad-microsoft-printnightmare-no-funciona-deshabilita-unico-parche-no-oficial-disponible?idU=3
https://www.ccn-cert.cni.es/seguridad-al-dia/alertas-ccn-cert/11081-ccn-cert-al-07-21-vulnerabilidad-en-microsoft.html