Olympus Winter & Ibe GmbH, Kuehnstraße 61, 22045 Hamburgo

A quien corresponda

Fecha
30.07.2021

PrintNightmare -
Vulnerabilidad de ejecución remota de código del Administrador de trabajos de impresión de Windows

Estimados señores y señoras:

Se ha detectado una vulnerabilidad crítica en el servicio Administrador de trabajos de impresión de Windows. Se ha llamado «Print-Nightmare». Microsoft asignó el número **CVE-2021-1675** a esta vulnerabilidad.

El 29 de junio de 2021, los *exploits* de la vulnerabilidad empezaron a circular. Microsoft asignó un segundo número a esta vulnerabilidad: **CVE-2021-34527**.

El 7 de julio de 2021, Microsoft lanzó actualizaciones fuera de banda para algunas (pero no todas) las versiones de Windows. Según el aviso sobre las actualizaciones de Microsoft, «las actualizaciones de seguridad lanzadas el 6 de julio de 2021 y posteriormente contienen protecciones contra CVE-2021-1675 y el *exploit* adicional de ejecución remota de código en el servicio Administrador de trabajos de impresión de Windows conocido como “PrintNightmare”, documentado en CVE-2021-34527». Se ha detectado la libre circulación de la explotación, y TODOS los sistemas Windows están afectados.

El 15 de julio de 2021, Microsoft asignó un tercer número a la vulnerabilidad PrintNightmare: **CVE-2021-34481**. Todavía no se conoce ningún *exploit* para esta vulnerabilidad.

Dispositivos OSTE afectados

Todas las versiones de los siguientes productos OSTE incluyen una versión de Windows y están afectados por la vulnerabilidad PrintNightmare:

- VMC-3
- VMC-7
- VMC-10
- VMC-30.

OSTE publicó el boletín de servicio SBU_100-219-293 para abordar la vulnerabilidad PrintNightmare en estos productos. Este boletín de servicio contiene instrucciones para que los ingenieros de servicio puedan detener y deshabilitar el servicio Administrador de trabajos de impresión en Windows para VMC-3, VMC-7, VMC-10 y VMC-30. Deshabilitar el servicio Administrador de trabajos de impresión de Windows es una solución rápida y eficaz para cerrar la vulnerabilidad PrintNightmare en Windows.

Póngase en contacto con el servicio de Olympus para aplicar en su VMC las medidas de corrección definidas en el boletín de servicio.

Otros productos OSTE

OSTE también produce y suministra software que debe instalarse en ordenadores con sistema operativo Windows:

- ENDOBASE
- Hytrack

Debido al alto riesgo de la vulnerabilidad PrintNightmare, OSTE recomienda encarecidamente aplicar las siguientes medidas de corrección para minimizar el riesgo causado por la vulnerabilidad PrintNightmare.

Recomendación general

La vulnerabilidad PrintNightmare afecta a todas las versiones y todos los tipos de Windows: instalaciones de cliente y servidor.

Si un ordenador Windows no necesita la funcionalidad de impresión, OSTE recomienda detener y deshabilitar el servicio Administrador de trabajos de impresión en dicho ordenador. Deshabilitar el servicio Administrador de trabajos de impresión evita la vulnerabilidad PrintNightmare en todas las versiones y todos los tipos de Windows. Sin embargo, también deshabilita la opción de imprimir de un ordenador.

La funcionalidad de impresión se necesita en los servidores Hytrack si deben imprimirse automáticamente los protocolos de reprocesado y en los clientes Hytrack, para la impresión manual de los protocolos

En los servidores ENDOBASE, la función de impresión no es necesaria.

En cuanto al tercer número CVE asociado a PrintNightmare, CVE-2021-34481, la única solución que ha dado Microsoft en la fecha de publicación del presente documento (julio de 2021) es deshabilitar el servicio Administrador de trabajos de impresión.

Hay más información disponible en la página web de Microsoft para CVE-2021-34481:

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34481

Si se necesita la impresión en un ordenador Windows, la medida de corrección recomendada dependerá de la versión de Windows.

Versiones de Windows 10 y de servidor basadas en Windows 10

Microsoft lanzó actualizaciones de seguridad para todas las versiones de Windows 10 y las versiones de servidor relacionadas. Hay información detallada y enlaces a los artículos de la base de conocimientos relacionados disponibles en la página web de Microsoft para CVE-2021-34527:

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

Además de la instalación de actualizaciones, para proteger su sistema, debe confirmar que la siguiente configuración del registro está establecida en 0 (cero) o sin definir:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint`
- `NoWarningNoElevationOnInstall = 0 (DWORD) o not defined (configuración predeterminada)`
- `UpdatePromptSettings = 0 (DWORD) o not defined (configuración predeterminada)`

Establecer `NoWarningNoElevationOnInstall` en 1 hace que su sistema sea vulnerable por diseño.

Versiones de Windows 7 y de servidor basadas en Windows 7

Microsoft lanzó actualizaciones de seguridad para versiones de Windows 7 y de servidor basadas en Windows 7 solo para clientes con un contrato de mantenimiento (*Extended Support Update*, ESU).

Si no hay opción de deshabilitar el servicio Administrador de trabajos de impresión, solo existen unas pocas soluciones para minimizar el riesgo creado por la vulnerabilidad PrintNightmare.

Deshabilitar la impresión remota entrante a través de la directiva de grupo

Configure los ajustes a través de la directiva de grupo como se indica a continuación:

`Computer Configuration / Administrative Templates / Printers`

Deshabilite la directiva «`Allow Print Spooler to accept client connections (Permitir que el administrador de trabajos de impresión acepte conexiones cliente)`» para bloquear ataques remotos.

Debe reiniciar el servicio Administrador de trabajos de impresión para que se aplique la directiva de grupo.

Hay información detallada disponible en la página web de Microsoft para CVE-2021-34527:

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

Restringir la instalación de nuevos controladores de impresora (ajustes de apuntar e imprimir)

Además, sin una actualización de seguridad instalada, se recomiendan los siguientes ajustes para mitigar el riesgo creado por la vulnerabilidad PrintNightmare:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint`
- `NoWarningNoElevationOnInstall = 0 (DWORD) o not defined (configuración predeterminada)`
- `UpdatePromptSettings = 0 (DWORD) o not defined (configuración predeterminada)`

Establecer `NoWarningNoElevationOnInstall` en 1 hace que su sistema sea vulnerable por diseño.

Atentamente,

Alois Baier
Director de Seguridad de los productos
I+D | Seguridad de los productos