BOLETÍN DE ALERTA

Boletín Nro.: 2022-24
Fecha de publicación: 31/05/2022
Tema: Vulnerabilidad de ejecución remota de código (RCE) en Microsoft Office.

Productos afectados:

- Microsoft Word, 2013 - 2021 (incluidas las versiones Professional Plus)
- Microsoft Office, 2013 - 2021 (incluidas las versiones Professional Plus)

Descripción:

Microsoft ha reportado un nuevo aviso de seguridad sobre una vulnerabilidad que afecta a archivos de Microsoft Office, que permitiría a un atacante realizar ejecución remota de código (RCE). La vulnerabilidad está siendo explotada activamente y existe una prueba de concepto (PoC) pública de la misma.

La vulnerabilidad denominada "Follina" fue asignada como CVE-2022-30190, con severidad alta y puntuación de 7.8. Esta se debe a una incorrecta validación de entrada al procesar archivos de Word en la funcionalidad para cargar HTML de un enlace externo y luego utiliza el esquema "ms-msdt" para ejecutar código Powershell. Un atacante remoto no autenticado podría aprovechar esta vulnerabilidad para realizar ejecución remota de código (RCE) en el sistema operativo de destino, incluso aunque los macros se encuentren deshabilitados.

Impacto:

La explotación de esta vulnerabilidad permitiría a un atacante realizar ejecución remota de código (RCE), podría instalar programas, ver, cambiar o eliminar datos, y crear cuentas en el contexto permitido por los derechos del usuario.

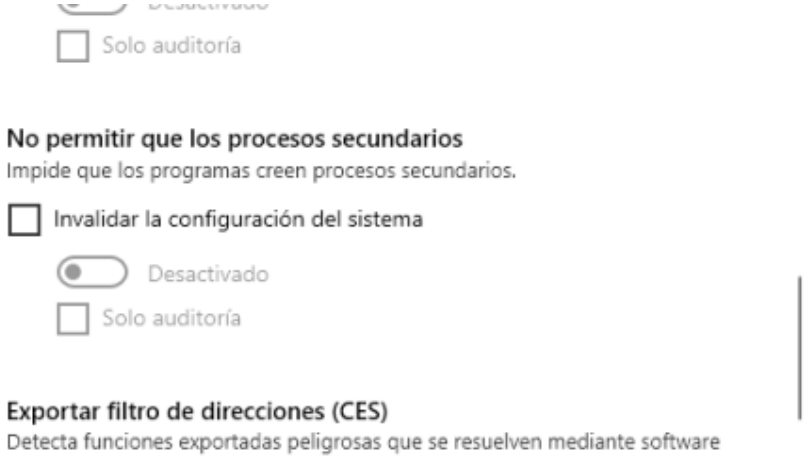
Detección y Protección:

1. Para usuarios con Microsoft Defender Antivirus activar la **protección entregada en la nube,** el **envío automático de muestras** y para los que usan.

El antivirus Microsoft Defender proporciona detecciones y protecciones bajo las siguientes firmas utilizando la compilación de detección **1.367.719.0** o más reciente:

- **Troyano:Win32/Mesdetty.A** (bloquea la línea de comandos msdt).
- **Troyano:Win32/Mesdetty.B** (bloquea la línea de comandos msdt).
- Comportamiento:Win32/MesdettyLaunch.A.
- Comportamiento:Win32/MesdettyLaunch.B.
- Comportamiento:Win32/MesdettyLaunch.C.

2. Para usuarios con Microsoft Defender for Endpoint, habilitar la **regla de reducción de la superficie de ataque** que impide que las aplicaciones de Office creen procesos secundarios.



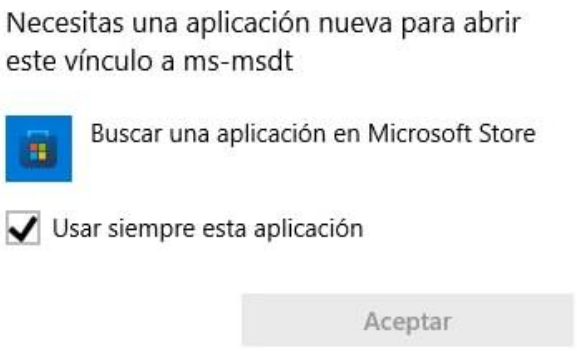
Microsoft Defender para Endpoint proporciona a los clientes detecciones y alertas. Los siguientes mensajes de alerta en el portal de Microsoft 365 Defender pueden indicar actividad ilícita en su red:

- **comportamiento sospechoso de una aplicación de Office,**
- **comportamiento sospechoso de Msdt.exe.**

Mitigación:

Actualmente Microsoft no ha publicado parches para CVE-2022-30190, sin embargo sugerimos seguir las siguientes instrucciones de mitigación para la vulnerabilidad:

1. Ejecutar el símbolo del sistema como administrador.
2. Realizar una backup de la clave **-HKEY_CLASSES_ROOT\ms-msdt** del regedit en caso de querer recuperar la asociación del enlace a posterior, mediante el comando **reg export HKEY_CLASSES_ROOT\ms-msdt filename**
3. Eliminar la clave del registro: **[-HKEY_CLASSES_ROOT\ms-msdt]**, mediante el comando **reg delete HKEY_CLASSES_ROOT\ms-msdt /f.** Una vez que la clave HKEY_CLASSES_ROOT\ms-msdt fuese eliminada del registro, si se intenta lanzar el ataque, el usuario verá el siguiente mensaje:



Importante: Los cambios se harán efectivos recién tras el reinicio.

Fuente: https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/

Información adicional:

- https://www.cybersecurity-help.cz/vdb/SB2022053005
- https://thehackernews.com/2022/05/watch-out-researchers-spot-new.html
- https://thehackernews.com/2022/05/microsoft-releases-workarounds-for.html
- https://support.microsoft.com/en-us/office/update-office-with-microsoft-update-f59d3f9d-bd5d-4d3b-a08e-1dd659cf5282
- https://twitter.com/nRoKzgz/status/1531556476526989312
- https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/
- https://www.helpnetsecurity.com/2022/05/31/cve-2022-30190-follina/
- https://empresas.blogthinkbig.com/lucha-windows-ciberseguridad-partevi/