Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

Follina Zero Day en Microsoft Office

31/mayo/2022

Contenido

INTRODUCCIÓN

Mediante este boletín, le informamos a nuestros clientes sobre una nueva vulnerabilidad de día cero en Microsoft Office, con el fin de que usted pueda estar al tanto sobre la vulnerabilidad y pueda aplicar acciones sobre ella.

Día Cero en Microsoft Office

A continuación, se encuentra en cuadro de identificación de la vulnerabilidad.

ID de alerta:	DSOC-CERT_2022_05_31
Clasificación de alerta:	Vulnerabilidad
Tipo de Impacto:	ALTO
TLP (Clasificación de información):	**WHITE**
Fecha de publicación:	05/31/2022
Es día cero (0 day):	NO

Resumen

Concretamente se trata de un fallo de Día cero que afecta a Office. Los piratas informáticos lo están utilizando para lanzar comandos maliciosos en PowerShell mediante la herramienta de diagnóstico de Microsoft, que se conoce como MSDT. Este fallo ha sido nombrado como Follina, aunque aún no tiene código de rastreo.

En caso de que un atacante ejecuta esta vulnerabilidad, podría abrir una puerta a un nuevo vector de ataque crítico que va a aprovecharse de Microsoft Office. No necesita permisos de administrador y además el antivirus de Windows no lo detecta como una amenaza. No necesita que se habilite las macros para ejecutarse.

¿Cómo podemos ser víctimas de este ataque?

Simplemente tendríamos que abrir un documento de Word y automáticamente podría ejecutar comandos maliciosos de PowerShell a través de MSDT. Según los investigadores de seguridad, detectaron esta vulnerabilidad de casualidad mientras analizaban otro fallo en VirusTotal.

Indicaron que utiliza un enlace externo de Word para cargar HTML y a partir de ahí usar el esquema ms-msdt para poder ejecutar el código de PowerShell.
El script de PowerShell lo que hará es extraer un archivo codificado en Base64 de un archivo RAR y posteriormente lo ejecutará. No obstante, indican que no está claro qué actividad maliciosa ha realizado este tipo de ataque.

Los investigadores dicen que, dependiendo de la carga útil, un atacante podría usar este exploit para llegar a ubicaciones remotas en la red de la víctima.

Esto permitiría a un atacante recopilar hashes de las contraseñas de la máquina Windows de la víctima que son útiles para actividades posteriores a la explotación.

La detección de esta vulnerabilidad es difícil:

Para detectar un ataque a través de este vector, Huntress apunta a monitorear los procesos en el sistema porque la carga útil de Follina crea un proceso secundario de 'msdt.exe' bajo el padre infractor de Microsoft Office.
Para las organizaciones que confían en las reglas de reducción de la superficie de ataque (ASR) de Microsoft Defender, Huntress recomienda activar " Bloquear todas las aplicaciones de Office para que no creen procesos secundarios " en el modo Bloquear, lo que evitaría las vulnerabilidades de Follina.

Solución alternativa disponible

Según Redmond, los administradores y usuarios pueden bloquear los ataques que explotan CVE-2022-30190 al deshabilitar el protocolo URL de MSDT, que los actores maliciosos usan para iniciar solucionadores de problemas y ejecutar código en sistemas vulnerables.

Para deshabilitar el protocolo URL de MSDT en un dispositivo Windows, debe realizar el siguiente procedimiento:

Ejecute el símbolo del sistema como administrador .

Para hacer una copia de seguridad de la clave de registro, ejecute el comando " *reg export HKEY_CLASSES_ROOT\ms-msdt ms-msdt.reg* "

Ejecute el comando " *reg delete HKEY_CLASSES_ROOT\ms-msdt /f* "

Después de que Microsoft publique un parche CVE-2022-30190, puede deshacer la solución alternativa iniciando un símbolo del sistema elevado y ejecutando el comando reg import ms-msdt.reg (nombre de archivo es el nombre de la copia de seguridad del registro creada al deshabilitar el protocolo).

Microsoft Defender Antivirus 1.367.719.0 o posterior ahora también viene con detecciones para una posible explotación de vulnerabilidades bajo las siguientes firmas:

Troyano:Win32/Mesdetty.A

Troyano:Win32/Mesdetty.B

Comportamiento: Win32/MesdettyLaunch.A

Comportamiento: Win32/MesdettyLaunch.B

Comportamiento: Win32/MesdettyLaunch.C

Si bien Microsoft dice que Vista protegida y Protección de aplicaciones de Microsoft Office bloquearían los ataques CVE-2022-30190, el analista de vulnerabilidades CERT/CC Will Dormann (y otros investigadores) descubrió que la característica de seguridad no bloqueará los intentos de explotación si el objetivo obtiene una vista previa de los documentos maliciosos en Explorador de Windows.

Por lo tanto, también se recomienda deshabilitar el panel de vista previa en el Explorador de Windows para eliminar también este vector de ataque.

Recomendaciones

1. Favor, no ejecutar documentos de Office de los cuales se desconozca su procedencia.
2. Mantenga su software Antivirus actualizado.
3. Asegurese de instalar las ultimas versiones de su sistema operativo.
4. Analizar si es viable en su entorno poder deshabilitar el protocolo URL de MSD, para que en caso de ejecutar un fichero infectado con carga maliciosa, esta no pueda proliferar.

Noticia Completa

https://www.redeszone.net/noticias/seguridad/fallo-dia-cero-office/

https://www.bleepingcomputer.com/news/microsoft/microsoft-shares-mitigation-for-office-zero-day-exploited-in-attacks/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757
El Salvador: +(503) 2249 4252
Honduras: +(504) 2283 5904
República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente