Píldora Informativa

GPIT
VIEM

Vulnerabilidad
FOLLINA y DOG WALK

No. 001

Universidad Nacional Abierta y a Distancia

UNAD
GRUPO FUNCIONAL DE SEGURIDAD INFORMATICA - GFSI
17/06/2022

FOLLINA

Fuente: https://www.indonations.com/2022/06/follina-0-day-flaw-microsoft-deploys.html

Todos los días la ciberseguridad es cambiante, aparece casi diariamente una nueva amenaza de algún tipo de ataque que tiene como consecuencia la pérdida de datos, pérdida de reputación o de efectivo, surgen así dos vulnerabilidades llamadas FOLLINA y DOG WALK. A finales de mayo de 2021 el investigador Kevin Beauman descubrió un EXPLOIT que denomino FOLLINA, este no fue detectado por Windows Defender, permite que un Documento de Word infectado utilice la función de plantilla remota de Word para recuperar un archivo HTML de un servidor web remoto, que a su vez utiliza el ms-msdt esquema Ms-Protocol URI para cargar Código y ejecutar "Power Shell". El "MSDT" en la descripción anterior se refiere a la infraestructura de Microsoft para ejecutar Solucionadores al problema. Pequeñas utilidades incluidas con Windows 10 y versiones posteriores (incluido Windows server 2019) que supuestamente lo ayudaron a resolver problemas comunes con dispositivo de sonido, impresoras, etc.

El resultado de esta vulnerabilidad de día cero de Microsoft: Abrir un documento infectado descargaría y ejecutaría POWER SHELL arbitrario elegido por el atacante en su máquina con Windows. UPS. En marzo de 2021 se informó a Microsoft de esta vulnerabilidad en Microsoft Teams, Microsoft solucionó el problema, pero solo en Teams; el problema resurgió en marzo de 2022 y a partir de junio 7 de 2022 Microsoft aún no ha lanzado un PARCHE. Agregaron las firmas de FOLLINA a las herramientas antivirus Defender Vulnerability Management y Defender.

FORMAS DE MITIGAR FOLLINA

El centro de seguridad de Microsoft contiene una mitigación manual:

- ✓ Elimine el subárbol de registro HKEY_CLASSES-ROOT /ms-msdt

Esto le permite ejecutar SOLUCIONADOR DE PROBLEMAS desde Windows. Pero no permite que se inicien a través de direcciones URL. El problema es que este es un paso manual.

El investigador propone crear una política de grupo y para deshabilitar la configuración que habilita el acceso al solucionador de problemas por completo: Cree una política en el editor de políticas de grupo y en el nodo configuración de la computadora, expanda plantillas administrativas > Sistema > Solución de problemas y Diagnósticos > Diagnósticos con secuencias de comandos > en esa categoría establezca Solución de problemas: permitir que los usuarios accedan y ejecuten los asistentes para la solución de problemas en "DESHABILITADO", luego distribuya la política según corresponda. Hasta

que Microsoft publique un PARCHE formal para las versiones afectadas de Windows y Office (Office versiones 2013.2016,2021; Office Pro-Plus y Office 365 en el canal semestral), esta mitigación es en la actualidad la mejor opción.

Microsoft sugiere que se puede usar DEFENDER para ENDPOINT para aplicar la regla: BLOQUEAR TODAS LAS APLICACIONES DE OFFICE PARA QUE NO CREEN PROCESOS SECUNDARIOS, en los casos en que hayan comprado las licencias que le permitan ejecutar DEFENDER para ENDPOINT.

DOG WALK

Es un exploit que fue informado a Microsoft en enero de 2020 por el investigador Imre Reid; Microsoft informó que no era una amenaza de seguridad real porque se requiere que la víctima abriera un archivo(.CAB) que contiene un archivo de configuración de diagnóstico).

MITIGACION DE DOG WALK

No existe en la actualidad mitigación para DOG WALK. Una solución efectiva requiere que Microsoft repare el subsistema MSDT para que no sea vulnerable al ataque de ruta transversal. Hay otras dos mitigaciones que Microsoft podría aplicar más rápido:

- ✓ Hacer que MSDT respete la bandera de "Marca de la WEB" que Windows usa para marcar los ejecutables que se descargaron de internet. Esta bandera es la razón por la cual el explorador de Windows l pregunta. ¿ESTA SEGURO QUE DESEA ABRIR ESTE ARCHIVO? cuando intenta abrir un archivo ejecutable que ha descargado desde su navegador.
- ✓ Agregue la detección de esta vulnerabilidad específica a DEFENDER y DEFENDER FOR ENDPOINT.
- ✓ Otra mitigación es la que proviene de la empresa denominada OPATCH, que fabrica una herramienta de parcheo en memoria que aplica lo que la empresa llama "microparches" a los ejecutables en ejecución. Una vez que instale el agente OPATCH, descargará parches para los ejecutables en su máquina, aplicándolos automáticamente cuando el ejecutable se ejecuta sin modificar la copia en el disco (evitando así la mayoría de los tipos de comprobaciones antimalware basadas en archivos).

GLOSARIO

DOG WALK: Es una vulnerabilidad 0-day para Windows que afecta todas las versiones de Windows 7 en adelante y Windows Server 2008 en adelante

Exploit: Es un ataque que se basa en la falencia del software o hardware encontrando vulnerabilidades a través de un software o una línea de código para tomar control del equipo o el robo de información

FOLLINA: Es una vulnerabilidad identificada por MITRE como CVE-2022-30190, se encuentra en la herramienta de Microsoft Windows Support Diagnostic Tool (MSDT), ya que su vulnerabilidad es a través de un documento de Office malicioso. Este documento cuenta con un archivo HTML que contiene un código JavaScript que ejecuta líneas de comandos a través de MSDT, una vez exitosa esta conexión los atacantes consiguen control del equipo y pueden instalar o desinstalar programas, ver, modificar, destruir, robar información.

Power Shell: Es una interfaz de línea de comandos o CLI (Command-Line Interface) que tiene la posibilidad de ejecutar Scripts (unión de comandos) y que facilita la configuración, administración y automatización de tareas multiplataforma

Windows Defender: Es un antivirus de seguridad de propiedad de Microsoft, para evitar ataques de virus, malware, pone en cuarentena archivos sospechosos o software malicioso

REFERENCIAS

Robichaux, P (2022) New Microsoft Zero-Day Vulnerability Times Two: Follina and DogWalk Practical 365. https://practical365.com/new-microsoft-zero-day-vulnerability-times-two-follina-and-dogwalk/

Nuevo Zero-Day RCE en Microsoft Office (aka 'Follina'), ya está siendo utilizado por atacantes. (2022) En https://www.cronup.com/nuevo-zero-day-rce-en-microsoft-office-aka-follina-ya-esta-siendo-utilizado-por-atacantes/

¿Qué es PowerShell? https://www.geeknetic.es/PowerShell/que-es-y-para-que-sirve

GPIT - Gerencia de plataformas e infraestructura tecnológica
VIEM – Vicerrectoría de Innovación y Emprendimiento
Seguridad Informática
Tel: 601-3443700 Ext 1610
UNAD