Se puso a disposición un parche de seguridad no oficial para una nueva vulnerabilidad de día cero de Windows en la Herramienta de Diagnóstico de Soporte de Microsoft (MSDT), incluso cuando la vulnerabilidad de Follina sigue siendo explotada en la naturaleza.

El problema, al que se hace referencia como DogWalk, se relaciona con una falla de cruce de ruta que se puede explotar para ocultar un archivo ejecutable malicioso en la carpeta de inicio de Windows cuando un objetivo potencial abre un archivo de almacenamiento «.diagcab» especialmente diseñado, que contiene un archivo de configuración de diagnóstico.

La idea es que la carga útil se ejecute la próxima vez que la víctima inicie sesión en el sistema después de un reinicio. La vulnerabilidad afecta a todas las versiones de Windows, desde Windows 7 y Server 2008 hasta las últimas versiones.

DogWalk fue revelado originalmente por el investigador de seguridad Imre Rad en enero de 2020, después de que Microsoft, habiendo reconocido el problema, no lo considerara como un problema de seguridad.

> *«Hay una serie de tipos de archivos que pueden ejecutar código de esta forma, pero técnicamente no son 'ejecutables'. Y varios de estos se consideran inseguros para que los usuarios los descarguen o reciban en el correo electrónico, incluso '.diagcab' está bloqueado de forma predeterminada en Outlook en la web y otros lugares»*, dijo Microsoft entonces.

Aunque todos los archivos descargados y recibidos por correo electrónico incluyen una etiqueta Mark-of-the-Web (MOTW) que se usa para determinar su origen y desencadenar una respuesta de seguridad adecuada, Mitja Kolsek de 0patch, dijo que la aplicación MSDT no está diseñada para verificar esta marca y por lo tanto, permite que el archivo .diagcab se abra sin previo aviso.

> *«Outlook no es el único vehículo de entrega: dicho archivo es descargado alegremente por todos los principales navegadores, incluido Microsoft Edge, simplemente visitando un sitio web, y solo se necesita un solo clic (o un clic incorrecto) en la lista de descargas del navegador para abrirlo»*, dijo Kolsek.

> *«No se muestra ninguna advertencia en el proceso, en contraste con la descarga y apertura de cualquier otro archivo conocido capaz de ejecutar el código del atacante».*

Los parches y el renovado interés en el error de día cero siguen a la explotación activa de la vulnerabilidad de ejecución remota de código Follina al aprovechar documentos de Word con malware que abusan del esquema URI del protocolo «ms-msdt:».

Según la compañía de seguridad Proofpoint, la vulnerabilidad (CVE-2022-30190, puntaje CVSS: 7.8) está siendo armada por un atacante rastreado como TA570 para entregar el troyano de robo de información QBot (también conocido como Qakbot).

> *«El actor usa mensajes secuestrados de hilo con archivos adjuntos HTLM, que si se abren, arrojan un archivo ZIP»,* dijo la compañía en una serie de tuits.

> *«El archivo contiene un IMG con un documento de Word, un archivo de acceso directo y una DLL. El LNK ejecutará la DLL para iniciar QBot. El documento cargará y ejecutará un archivo HTML que contiene un archivo PowerShell que abusa de CVE-2022-30190 utilizado para descargar y ejecutar QBot»*.

QBot también ha sido empleado por corredores de acceso inicial para obtener acceso inicial a

las redes de destino, lo que permite a los afiliados de ransomware abusar del punto de apoyo para implementar malware de cifrado de archivos.

El informe DFIR, a inicios del año, también documentó cómo las infecciones de QBot se mueven rápidamente, lo que permite que el malware recolecte datos del navegador y correos electrónicos de Outlook apenas 30 minutos después del acceso inicial y propague la carga útil a una estación de trabajo adyacente alrededor de la marca de 50 minutos.