Microsoft publicó este lunes una guía para una vulnerabilidad de día cero recientemente descubierta en su paquete de productividad de Office, que podría explotarse para lograr la ejecución de código en los sistemas afectados.

La vulnerabilidad, rastreada como CVE-2022-30190, tiene una calificación de 7.8 sobre 10. Las versiones de Microsoft Office 2013, Office 2016, Office 2019 y Office 2021, así como las ediciones Professional Plus, se ven afectadas.

> *«Para ayudar a proteger a los clientes, hemos publicado CVE-2022-30190 y orientación adicional aquí«*, dijo un portavoz de Microsoft.

La vulnerabilidad de Follina, que se dio a conocer a fines de la semana pasada, involucró un exploit del mundo real que aprovechó la deficiencia en un documento de Word armado para ejecutar código de PowerShell arbitrario, haciendo uso del esquema URI *«ms-msdt»*. La muestra se subió a VirusTotal desde Bielorrusia.

Pero los primeros signos de explotación de la falla se remontan al 12 de abril de 2022, cuando se cargó una segunda muestra a la base de datos de malware. Se cree que esta pieza apuntó a un usuario en Rusia con un documento de Word malicioso («приглашение на интервью.doc«) que se hizo pasar por una invitación a una entrevista con Sputnik Radio.

> *«Existe una vulnerabilidad de ejecución remota de código cuando se llama a MSDT utilizando el protocolo URL desde una aplicación de llamada como Word»,* dijo Microsoft en un aviso.

> *«Un atacante que explota con éxito esta vulnerabilidad puede ejecutar código arbitrario con los privilegios de la aplicación que llama. El atacante puede después instalar programas, ver, cambiar o eliminar datos, o crear nuevas cuentas en el*

> *contexto permitido por los derechos del usuario»*.

La compañía otorgó el crédito a Crazyman, miembro de Shadow Chaser Group, por informar sobre la vulnerabilidad el 12 de abril, coincidiendo con le descubrimiento del exploit en estado salvaje dirigido a los usuarios rusos, lo que indica que la compañía ya estaba al tanto de la vulnerabilidad.

De hecho, según las capturas de pantalla compartidas por el investigador en Twitter, Microsoft cerró el informe de envío de vulnerabilidades el 21 de abril de 2022, indicando que *«el problema se solucionó»,* al mismo tiempo que descartó la falla como *«no un problema de seguridad»* ya que requiere una clave de acceso proporcionada por un técnico de soporte al iniciar la herramienta de diagnóstico.

Además de publicar reglas de detección para Microsoft Defender para Endpoint, la empresa ofreció soluciones alternativas en su guía para deshabilitar el protocolo URL de MSDT a través de una modificación del Registro de Windows.

> *«Aunque la aplicación que llama es una aplicación de Microsoft Office, de forma predeterminada, Microsoft Office abre documentos de Internet en vista protegida o protección de aplicaciones para Office, los cuales evitan el ataque actual»,* dijo Microsoft.

Esta no es la primera vez que los esquemas de protocolo de Microsoft Office como *«ms-msdt»* se someten al análisis por su posible uso indebido. A inicios de enero, la empresa alemana de ciberseguridad SySS reveló cómo es posible abrir archivos directamente por medio de URL especialmente diseñadas como *«ms-excel:ofv|u|https://192.168.1.10/poc[.]xls»*.