La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA) añadió el jueves una vulnerabilidad de seguridad de severidad media, que afecta a Microsoft Windows, a su catálogo de Vulnerabilidades Conocidas y Explotadas (KEV, por sus siglas en inglés), tras confirmarse que ya está siendo aprovechada activamente por atacantes.

Esta vulnerabilidad, identificada como CVE-2025-24054 (con una puntuación CVSS de 6.5), corresponde a un fallo de suplantación que permite la filtración de hashes NTLM (New Technology LAN Manager). Microsoft ya había corregido este fallo el mes pasado en sus actualizaciones regulares del segundo martes (Patch Tuesday).

NTLM es un protocolo de autenticación antiguo que Microsoft dejó de recomendar oficialmente el año pasado en favor de Kerberos. En los últimos años, los atacantes han encontrado múltiples formas de explotar NTLM, como los ataques *pass-the-hash* y los ataques de retransmisión, para obtener estos hashes y usarlos en compromisos posteriores.

Según CISA:

> *«Microsoft Windows NTLM contiene una vulnerabilidad relacionada con el control externo de nombres de archivos o rutas, lo que permite a un atacante no autorizado realizar una suplantación a través de la red.»*

Microsoft explicó en marzo que esta vulnerabilidad puede activarse con solo una interacción mínima, por ejemplo, al hacer clic una vez, hacer clic derecho o realizar alguna acción sobre un archivo `.library-ms`, sin necesidad de abrirlo o ejecutarlo.

El hallazgo de esta falla fue atribuido a los investigadores Rintaro Koike de NTT Security Holdings, 0x6rss y j00sean.

Aunque Microsoft indicó que es poco probable que se explote (clasificada como “Exploitation Less Likely”), desde el 19 de marzo, la empresa de ciberseguridad Check Point confirmó que ya se está usando activamente. Los atacantes pueden usarla para obtener hashes NTLM o

contraseñas de usuario y acceder a sistemas internos.

Entre el 20 y 21 de marzo de 2025, se detectó una campaña dirigida a instituciones gubernamentales y privadas en Polonia y Rumania. En ese caso, los atacantes utilizaron *malspam* (correos maliciosos) con un enlace de Dropbox que contenía un archivo comprimido. Dicho archivo explotaba varias vulnerabilidades, incluida la CVE-2025-24054, para extraer hashes NTLMv2-SSP.

Se cree que esta vulnerabilidad es una variante de la CVE-2024-43451 (también con una puntuación CVSS de 6.5), corregida en noviembre de 2024, y que también ha sido utilizada en ataques contra Ucrania y Colombia por grupos como UAC-0194 y Blind Eagle.

Según Check Point, los atacantes distribuyen archivos en formato ZIP. Al ser descomprimidos, Windows Explorer intenta autenticarse vía SMB con un servidor remoto, filtrando automáticamente el hash NTLM del usuario sin que este realice acción alguna.

En una campaña más reciente, observada el 25 de marzo de 2025, los atacantes enviaron directamente un archivo llamado “Info.doc.library-ms” sin comprimirlo. Desde el primer ataque, se han identificado al menos 10 campañas con el objetivo de obtener hashes NTLM de las víctimas.

Check Point señaló:

> *«Estos ataques se basan en archivos `.library-ms` maliciosos para recolectar hashes NTLMv2 y facilitar movimientos laterales y escalamiento de privilegios dentro de las redes comprometidas.»*

Esta rápida explotación demuestra la urgencia de que las organizaciones apliquen los parches lo antes posible y revisen cómo manejan las vulnerabilidades relacionadas con NTLM. Dado que el ataque requiere una interacción mínima y permite a los atacantes obtener acceso a credenciales, representa una amenaza seria, especialmente por la posibilidad de

usar esos hashes en ataques *pass-the-hash*.

Por último, las agencias del Poder Ejecutivo Civil Federal (FCEB) deben corregir esta vulnerabilidad antes del 8 de mayo de 2025, debido a que ya está siendo explotada activamente.