Investigadores en ciberseguridad han identificado un caso de *«autenticación forzada»* que podría ser explotado para revelar los tokens NT LAN Manager (NTLM) de un usuario de Windows al engañar a la víctima para que abra un archivo específicamente creado en Microsoft Access.

Este ataque se vale de una característica legítima en la solución de gestión de bases de datos que permite a los usuarios enlazarse con fuentes de datos externas, como una tabla remota de SQL Server.

> Haifei Li, investigador de seguridad de Check Point, explicó: *«Esta característica puede ser utilizada por los atacantes para filtrar automáticamente los tokens NTLM del usuario de Windows hacia cualquier servidor controlado por el atacante, a través de cualquier puerto TCP, como el puerto 80. El ataque puede ser ejecutado siempre que la víctima abra un archivo .accdb o .mdb. De hecho, cualquier tipo de archivo de Office más común (como un .rtf) puede funcionar también».*

NTLM, un protocolo de autenticación introducido por Microsoft en 1993, es un protocolo de desafío-respuesta utilizado para autenticar a los usuarios durante el inicio de sesión. A lo largo del tiempo, se ha demostrado que es vulnerable a ataques como fuerza bruta, pass-the-hash y relay.

El ataque en cuestión abusa de la función de tabla vinculada en Access para filtrar los hashes NTLM a un servidor controlado por el atacante, al incrustar un archivo .accdb con un enlace a una base de datos remota de SQL Server dentro de un documento de MS Word, utilizando un mecanismo conocido como Object Linking and Embedding (OLE).

> *«Un atacante puede configurar un servidor bajo su control, escuchando en el puerto 80, e ingresar su dirección IP en el campo 'alias de servidor' mencionado anteriormente. Luego, pueden enviar el archivo de la base de datos, incluida la tabla vinculada, a la víctima»,* detalló Li.

Si la víctima abre el archivo y selecciona la tabla vinculada, el cliente de la víctima se comunica con el servidor controlado por el atacante para la autenticación, permitiendo a este último llevar a cabo un ataque de relay al iniciar un proceso de autenticación con un servidor NTLM específico dentro de la misma organización.

El servidor malicioso recibe el desafío, lo transmite a la víctima y obtiene una respuesta válida, la cual es finalmente enviada al remitente que desafía al CV como parte del proceso de autenticación controlado por el atacante CV↔ SA, recibe una respuesta válida y luego transmite esa respuesta al servidor NTLM.

A pesar de que Microsoft ha lanzado medidas para abordar este problema en la versión de Office/Access (Canal Actual, versión 2306, compilación 16529.20182) después de una divulgación responsable en enero de 2023, 0patch ha lanzado soluciones no oficiales para Office 2010, Office 2013, Office 2016, Office 2019 y Office 365.

Este desarrollo también coincide con el anuncio de Microsoft de sus planes de discontinuar NTLM en Windows 11 en favor de Kerberos para mejorar la seguridad.