Microsoft ha comunicado su intención de eliminar el Administrador de Red NT (NTLM) en futuras versiones de Windows 11, a medida que se orienta hacia métodos alternativos de autenticación y refuerza la seguridad.

> *«Nos enfocamos en fortalecer el protocolo de autenticación Kerberos, que ha sido el predeterminado desde el año 2000, y reducir la dependencia en el Administrador de Red NT (NTLM). Las novedades en Windows 11 incluyen la Autenticación Inicial y la Autenticación de Paso con Kerberos (IAKerb) y un Centro de Distribución de Claves (KDC) local para Kerberos»*, menciona la empresa tecnológica.

IAKerb permite a los clientes autenticarse con Kerberos en una amplia variedad de configuraciones de red. La segunda característica, un Centro de Distribución de Claves (KDC) local para Kerberos, amplía el soporte de Kerberos a cuentas locales.

El NTLM, introducido por primera vez en la década de 1990, es un conjunto de protocolos de seguridad diseñados para proporcionar autenticación, integridad y confidencialidad a los usuarios. Es una herramienta de inicio de sesión único (SSO) que se basa en un protocolo de desafío-respuesta que demuestra a un servidor o controlador de dominio que un usuario conoce la contraseña asociada a una cuenta.

Desde el lanzamiento de Windows 2000, el NTLM ha sido reemplazado por otro protocolo de autenticación llamado Kerberos, aunque el NTLM continúa utilizándose como mecanismo de respaldo.

> *«La principal diferencia entre el NTLM y Kerberos radica en cómo gestionan la autenticación. El NTLM se basa en un saludo de tres pasos entre el cliente y el servidor para autenticar a un usuario. Kerberos utiliza un proceso de dos partes que aprovecha un servicio de concesión de tickets o un centro de distribución de claves»,* señala CrowdStrike.

Otra distinción crucial es que mientras el NTLM se basa en el cifrado de contraseñas, el Kerberos utiliza la encriptación.

Además de las debilidades de seguridad intrínsecas del NTLM, la tecnología ha quedado expuesta a ataques de retransmisión, lo que podría permitir a actores maliciosos interceptar intentos de autenticación y obtener acceso no autorizado a recursos de red.

Microsoft también ha informado que está trabajando en abordar instancias de NTLM codificadas en sus componentes en preparación para la eliminación definitiva del NTLM en Windows 11, y agrega que está realizando mejoras que promueven el uso de Kerberos en lugar del NTLM.

> *«Todos estos cambios se habilitarán de manera automática y no requerirán configuración en la mayoría de los casos. El NTLM seguirá estando disponible como recurso de respaldo para mantener la compatibilidad existente»,* expresó Matthew Palko, líder principal de gestión de productos de Microsoft en la sección de Enterprise y Seguridad.