Investigadores en ciberseguridad han identificado que la política de grupo de Microsoft Active Directory, diseñada para desactivar NT LAN Manager (NTLM) v1, puede ser fácilmente burlada debido a una configuración incorrecta.

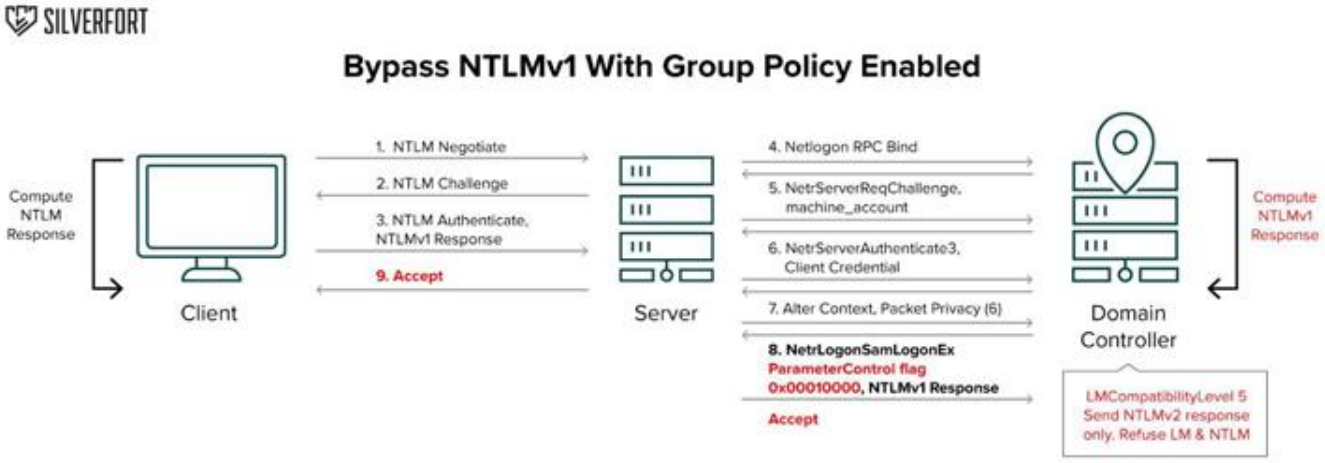
> *«Una simple mala configuración en aplicaciones locales puede invalidar la política de grupo, lo que neutraliza la medida destinada a impedir las autenticaciones NTLMv1»,* explicó Dor Segal, investigador de Silverfort, en un informe.

NTLM sigue siendo un método ampliamente empleado, especialmente en entornos Windows, para autenticar usuarios en una red. Aunque este protocolo obsoleto se mantiene por razones de compatibilidad con versiones anteriores, fue oficialmente declarado en desuso a mediados de 2024.

Hacia finales del año pasado, Microsoft eliminó NTLMv1 de forma oficial en Windows 11, versión 24H2, y en Windows Server 2025. Aunque NTLMv2 implementa mitigaciones que dificultan los ataques de retransmisión, la tecnología continúa presentando vulnerabilidades que han sido aprovechadas por atacantes para acceder a información sensible.

El método de explotación consiste en forzar a una víctima a autenticarse en un punto arbitrario o retransmitir las credenciales de autenticación hacia un objetivo vulnerable, permitiendo realizar acciones maliciosas en nombre de la víctima.

> *«La política de grupo de Microsoft está diseñada para deshabilitar NTLMv1 en toda la red. La clave de registro LMCompatibilityLevel evita que los controladores de dominio procesen mensajes NTLMv1, devolviendo un error de contraseña incorrecta (0xC000006A) cuando se intenta autenticar con NTLMv1″,* señaló Segal



Sin embargo, la investigación de Silverfort reveló que es posible evitar esta política y utilizar NTLMv1 mediante una configuración en el protocolo remoto de Netlogon (MS-NRPC).

En particular, la vulnerabilidad se encuentra en una estructura de datos denominada *NETLOGON_LOGON_IDENTITY_INFO*, que incluye un campo llamado *ParameterControl*. Este campo permite configurar la opción «Permitir autenticación NTLMv1 (MS-NLMP) incluso cuando solo se permite NTLMv2 (NTLM)».

> *«Nuestro análisis demuestra que las aplicaciones locales pueden ser configuradas para habilitar NTLMv1, anulando el nivel más alto de autenticación configurado en las políticas de Active Directory»,* destacó Segal.
>
> *«Esto implica que las organizaciones creen estar implementando correctamente la política de grupo, pero aplicaciones configuradas incorrectamente pueden seguir permitiendo el uso de NTLMv1».*

Para reducir los riesgos asociados con NTLMv1, es fundamental habilitar los registros de auditoría para todas las autenticaciones NTLM en el dominio y prestar especial atención a

aplicaciones que requieran mensajes NTLMv1. Asimismo, es crucial mantener todos los sistemas actualizados.

Este descubrimiento se suma al reporte del investigador Haifei Li sobre un *«comportamiento de día cero»* en archivos PDF, detectado en el entorno real, que podría filtrar información de *net-NTLM* al abrirse en Adobe Reader o Foxit PDF Reader bajo ciertas condiciones. Foxit Software corrigió esta vulnerabilidad en la versión 2024.4 para Windows.

Además, otro informe del investigador Alessandro Iandoli, de HN Security, detalla cómo algunas funciones de seguridad en Windows 11 (anteriores a la versión 24H2) podrían ser eludidas para lograr la ejecución de código arbitrario a nivel del núcleo del sistema.