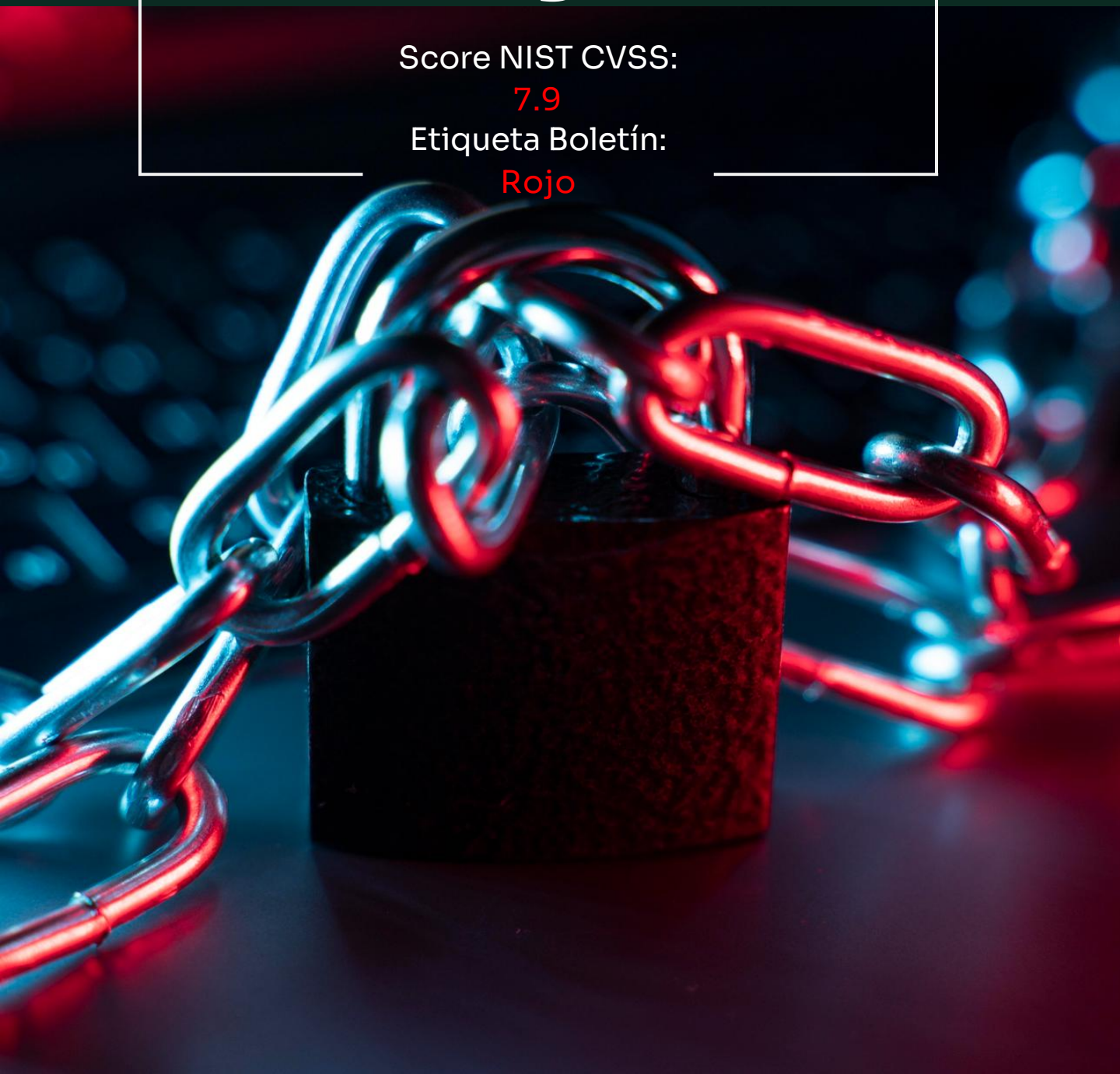
NESEC

ALWAYS SECURE, *NEVER AT RISK*

Boletín de ciberseguridad

Score NIST CVSS:
7.9
Etiqueta Boletín:
Rojo



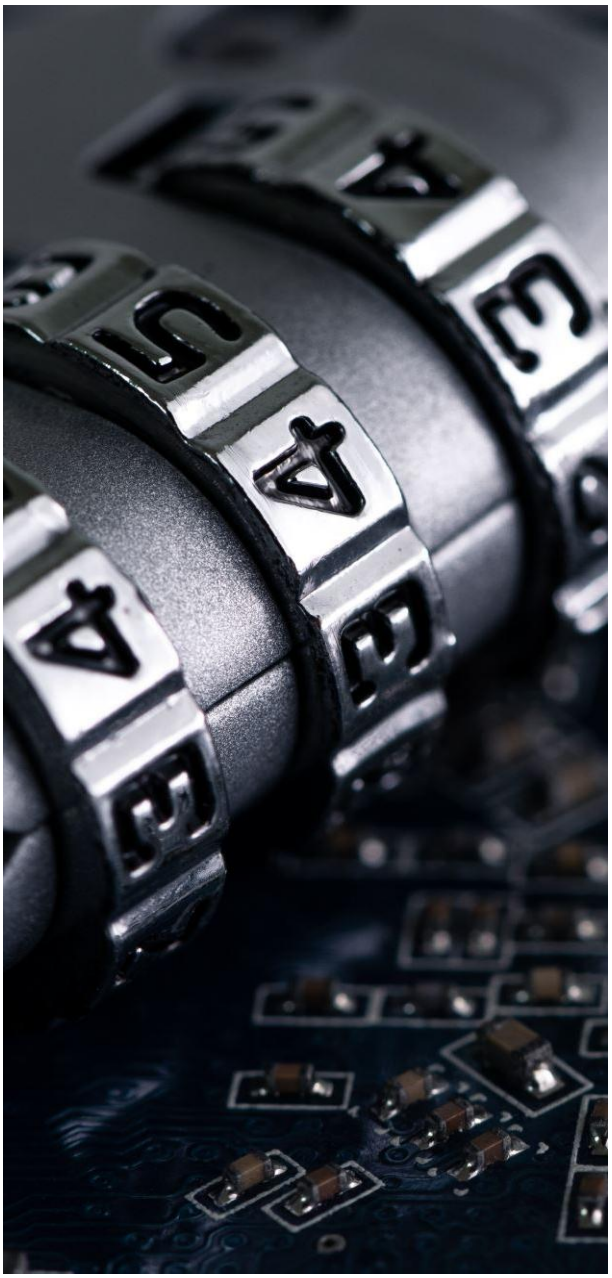
Zero Day de Windows: Robo de credenciales NTLM

Una nueva vulnerabilidad de día cero en NTLM permite a los atacantes robar las credenciales de NTLM haciendo que un usuario vea un archivo malicioso en el Explorador de Windows.

Esta vulnerabilidad afecta a todas las versiones de Windows, desde Windows 7 hasta Windows 11 y Server 2022. La falla puede aprovecharse para ataques de retransmisión de autenticación o ataques de diccionario.

Las estrategias de mitigación incluyen habilitar la protección ampliada para la autenticación, reforzar las configuraciones de LDAP y hacer la transición a protocolos de autenticación modernos como Kerberos.

Además, Microsoft solucionó una vulnerabilidad crítica de Windows 11 (CVE-2024-30085) que permitía aumentar los privilegios a nivel del sistema e instar a los usuarios a actualizar sus sistemas.



Impacto:

La explotación de este evento representa un riesgo grave para las cuentas de usuario, ya que expone nombres de usuario y contraseñas en texto claro. Si es aprovechada con éxito, podría llevar a un compromiso total del sistema, permitiendo a los atacantes acceder de manera no autorizada a sistemas, datos y redes sensibles.

Este Zero Day afecta a todas las versiones de Windows, desde Windows 7 hasta Windows 11 24H2, incluyendo Windows Server 2022.

Vulnerabilidades:

CVE-2024-30085: Vulnerabilidad de elevación de privilegios del controlador de mini filtro de Windows Cloud Files

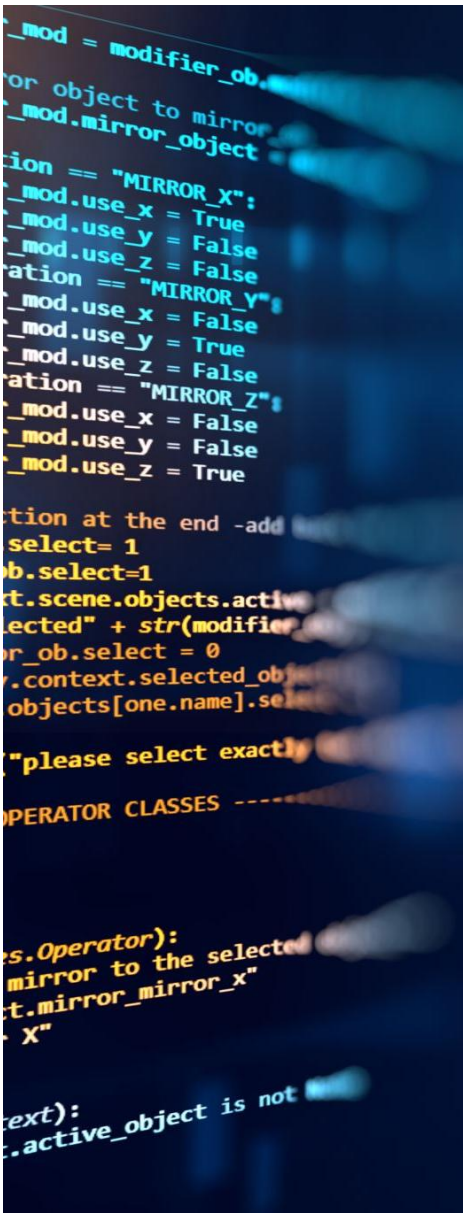
Activos :

- Microsoft Exchange Server
- Microsoft Windows
- Microsoft Windows Server

MITRE ATT&CK TTPs:

- T1203: Exploitation for Client Execution; Exploitation
- T1557: Adversary-in-the-Middle; Actions & Objectives

Modus operandi:
Robo de credenciales NTLM



Los atacantes explotan esta vulnerabilidad NTLM diseñando archivos maliciosos que contienen enlaces SMB incrustados, los cuales apuntan a servidores bajo su control. Estos archivos pueden ser distribuidos a través de correos de phishing, enlaces en sitios web comprometidos o mediante mensajería directa.

Al ser visualizados en el Explorador de Windows, **incluso sin ser abiertos**, los archivos activan automáticamente una solicitud de autenticación NTLM hacia el servidor del atacante. Durante esta interacción, Windows envía un hash NTLM de las credenciales del usuario al servidor malicioso.

Este hash puede ser utilizado por el atacante para realizar un ataque de "Pass-the-Hash", permitiendo el acceso no autorizado a recursos internos de la red.

Vector de ataque: Robo de credenciales NTLM

Preparación del archivo malicioso

- El atacante crea un archivo con enlaces SMB incrustados que apuntan a un servidor C2

Distribución del archivo malicioso

- El archivo es enviado a la victima.

Interacción de la victima

- La victima visualiza el archivo en el Explorador de Windows. No es necesario abrir el archivo.

Activación del enlace SMB

- Windows intenta cargar el recurso remoto referenciado en el archivo.

Captura de credenciales NLTM

- El servidor malicioso recibe el hash NTLM de las credenciales del usuario.

¿Qué hacer?

Para mitigar esta vulnerabilidad, Microsoft ha actualizado las directrices para habilitar la Protección Extendida para la Autenticación (EPA) en LDAP, AD CS y Exchange Server. En Windows Server 2022 y 2019, los administradores pueden habilitar manualmente EPA para AD CS y vinculación de canales para LDAP. Además, se recomienda actualizar a Windows Server 2025, ya que esta versión incluye EPA y vinculación de canales habilitados por defecto.

En caso de que algunas organizaciones dependan de NTLM por sistemas heredados, se sugiere implementar capas adicionales de autenticación, como políticas dinámicas basadas en riesgos, para proteger estos sistemas. No obstante, te compartimos estas recomendaciones adicionales:

- Habilita la protección extendida para la autenticación (EPA) en LDAP, Active Directory Certificate Services (AD CS) y Exchange Server para mitigar la vulnerabilidad de NTLM.
- Usa la política de grupo para auditar y restringir la autenticación NTLM a fin de reducir el riesgo de filtración de credenciales NTLM.
- Realiza la transición de **NTLM a Kerberos** e implemente la autenticación multifactor (MFA) para mejorar la seguridad.
- Aplica inmediatamente la actualización de Windows de diciembre de 2024 al parche **CVE-2024-30085.**
- Restringe el acceso administrativo solo a los usuarios de confianza.
- Supervisa la actividad del sistema para detectar comportamientos inusuales, especialmente en relación con las operaciones de archivos y los puntos de análisis.
- Emplea sistemas de detección de intrusos (IDS) para monitorear las señales de vulnerabilidades.

Fuentes de información.

1. How to Protect Your Environment From the NTLM Vulnerability
2. Windows 11 Privilege Escalation Vulnerability Lets Attackers Execute Code to Gain Access
3. Windows NTLM Credential Zero-Day Vulnerability Alert
4. NTLM Nightmare: New Vulnerability Leaves Windows Users Exposed

Boletín de ciberseguridad

Etiqueta Boletín:

Rojo

+52 (55) 8525 4111

info@onesec.mx
support@onesec.mx
sales@onesec.mx

SAN JACINTO NO. 8
COL. SAN ÁNGEL, C.P. 01000
ALCALDÍA ÁLVARO OBREGÓN, CDMX.

LINKEDIN | INSTAGRAM

PRESENCIA EN: CDMX | MONTERREY | GUADALAJARA