Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°024	Fecha: 28-01-2024
		Página: 4 de 11

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Los investigadores descubren cómo sus contraseñas NTLM podrían filtrarse a través de vulnerabilidades de Outlook		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. **ANTECEDENTES**:

Una laguna de ciberseguridad en Microsoft Outlook que se solucionó recientemente permitió a los actores de amenazas acceder a contraseñas hash de NT LAN Manager (NTLM) v2 abriendo un documento diseñado de forma exclusiva.

Identificado como CVE-2023-35636 con una puntuación CVSS de 6,5, Microsoft resolvió este problema como parte de sus actualizaciones del martes de parches implementadas en diciembre de 2023.

NTLM v2 es un protocolo criptográfico utilizado por Microsoft Windows para autenticar usuarios en servidores remotos. A pesar de ser más seguro que su predecesor, NTLM v2 sigue siendo vulnerable a ataques de retransmisión de autenticación y de fuerza bruta fuera de línea.

2. **DETALLES:**

"Un atacante podría aprovechar esta vulnerabilidad enviando un archivo cuidadosamente elaborado por correo electrónico y persuadiendo al usuario para que lo abra", afirmó Microsoft en un comunicado emitido el mes anterior.

Al utilizar una estrategia de ataque basada en web, un atacante podría alojar o utilizar un sitio web comprometido que acepte o muestre contenido generado por el usuario para presentar un archivo diseñado explícitamente para explotar esta vulnerabilidad".

La raíz de CVE-2023-35636 es la función para compartir calendario en el cliente de correo electrónico Outlook. Un mensaje de correo electrónico dañino se compone de la integración de dos encabezados conocidos como "Content-Class" y "x-sharing-config-url", en los cuales se puede manipular los valores para conectarse y compartir contenido a una máquina externa. Esta conectividad puede ser utilizada para interceptar el hash NTLMv2.

Supongamos que un atacante consigue extraer los hashes de NTLM. En ese caso, hay dos posibles métodos de ataque, que son los ataques de fuerza bruta sin conexión, que pueden revelar la contraseña original, y los ataques de retransmisión de autenticación, en los que una solicitud de autenticación a un servidor puede ser manipulada por el atacante con el hash NTLMv2 y conseguir autenticarse en el servidor bajo el nombre de la víctima.

Según Dolev Taler, un investigador de seguridad de Varonis que descubrió e informó el error, los hashes NTLM se pueden exponer utilizando el Analizador de rendimiento de Windows (WPA) y el Explorador de archivos de Windows, dos métodos de ataque que actualmente no se abordan.

"NTLM v2 normalmente se emplea cuando se autentica contra servicios basados en direcciones IP internas. Sin embargo, cuando el hash NTLM v2 se transmite a través de Internet, se vuelve vulnerable a ataques de retransmisión y de fuerza bruta fuera de línea".

3. **RECOMENDACIONES:**

- Actualizar el producto afectado a la última versión de software disponible que Microsoft lanzó en los parches el 12 de diciembre de 2023 para abordar esta vulnerabilidad.
- Habilitar la firma SMB, de tal manera que, al intentar modificar un mensaje SMB, el destinatario pueda detectar el cambio y rechazar el mensaje.
- Bloquear NTLM v2 saliente, especialmente en Windows 11 (25951) y versiones posteriores. Si es posible, aplicar la autenticación Kerberos y bloquear NTLM v2 tanto en el nivel de red como de aplicación.

Fuente de Información:	• hxxps://hackarizona.org/researchers-discover-how-your-ntlm-passwords-could-be-leaked-through-outlook-vulnerabilities/ • hxxps://blog.elhacker.net/2024/01/vulnerabilidad-en-microsoft-outlook-extraer-hash-passwords-ntlm-v2.html