DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°058**	**Fecha: 07-03-2024**
		Página: 6 de 12

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad en Microsoft Streaming utilizada en ciberataques de malware		
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:

Se ha reportado una vulnerabilidad de severidad **ALTA** de tipo desreferencia de puntero no confiable del servicio de Streaming de Microsoft (MSKSSRV.SYS) que está siendo explotada en ataques de malware. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante local obtener privilegios de SYSTEM en ataques de baja complejidad.

2. DETALLES:

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2023-29360, podría permitir a un atacante local obtener privilegios de SYSTEM en ataques de baja complejidad que no requieren la interacción del usuario.

Cabe indicar que la vulnerabilidad fue descubierta por Thomas Imbert de Synactiv en el Microsoft Streaming Service Proxy (MSKSSRV.SYS) y reportado a Microsoft a través de la Iniciativa Día Cero de Trend Micro. Microsoft corrigió el error durante el martes de parches de junio de 2023, y el código de explotación de prueba de concepto se lanzó en GitHub el 24 de septiembre del 2023.

La Agencia de Ciberseguridad e Infraestructura de EE. UU. (CISA) no ha detallado los ataques en curso, confirmó que no hay evidencia de su uso en ataques de Ransomware. La agencia también agregó el error a su Catálogo de vulnerabilidades explotadas conocidas, advirtió que dichos errores de seguridad son "vectores de ataque frecuentes para actores cibernéticos maliciosos y representan riesgos significativos para todas las entidades públicas y privadas.

Asimismo, la empresa de ciberseguridad Check Point, reveló que el malware Raspberry Robin ha estado explotando la vulnerabilidad CVE-2023-29360 desde agosto de 2023. Este malware, vinculado a múltiples grupos de cibercriminales, incluidos EvilCorp y la banda de ransomware Clop, se propaga principalmente a través de dispositivos USB y ha sido detectado en redes de diversas industrias desde su aparición en 2021. Desde su descubrimiento, este gusano ha evolucionado continuamente, adoptando nuevas tácticas de entrega y agregando nuevas características, incluida una evasión en la que arroja cargas útiles falsas para engañar a los investigadores.

A. Productos afectados:

Las siguientes plataformas basados en sistemas de 32 bits, sistemas basados en x64 y sistemas basados en ARM64 se ven afectados:

- Windows 10 y 11;
- Windows Server 2016 a Server 2022.

3. RECOMENDACIÓN:

- Parchear los equipos con sistemas Windows para abordar la vulnerabilidad en el Servicio de Streaming de Microsoft (MSKSSRV.SYS) que está siendo explotada activamente en ataques de malware. Cabe indicar que el parche para esta vulnerabilidad se publicó en junio del 2023.

Fuente de Información:	• hxxps://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29360 • hxxps://www.bleepingcomputer.com/news/security/cisa-warns-of-microsoft-streaming-bug-exploited-in-malware-attacks/