CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Vulnerabilidad de Software

Fecha: 24/06/2023

Problemática: Vulnerabilidad de omisión de la función de seguridad Mark of the Web (MOTW) de Microsoft Windows

Correlativo: AC-0048

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

Microsoft emitió un comunicado para informar a sus clientes sobre las vulnerabilidades identificadas como CVE-2022-41049 y CVE-2022-41091 respectivamente, que afectan a la función de seguridad Mark of the Web (MOTW) en sistemas operativos Microsoft Windows.

SITUACIÓN

Un atacante puede crear un archivo malicioso que evadiría las defensas de Mark of the Web (MOTW), lo que daría como resultado una pérdida limitada de integridad y disponibilidad de funciones de seguridad como Vista protegida en Microsoft Office, que se basan en el etiquetado MOTW.

Nivel de priorización

Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
Urgente	**Preventiva**

Matriz de Evaluación

Riesgo Alto/ Medio/ Bajo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
Alto	**Alta**	**Alta**	**Media**

RECOMENDACIONES

- Microsoft exhorta a sus clientes a realizar las actualizaciones correspondientes mara mitigar las vulnerabilidades identificadas.
- Considere implementar planes de recuperación ante desastres de TI que contengan procedimientos para realizar copias de seguridad de datos periódicas que se puedan usar para restaurar datos de la organización. Asegúrese de que las copias de seguridad se almacenen fuera del sistema y estén protegidas de los métodos comunes que los adversarios pueden usar para obtener acceso y destruir las copias de seguridad para evitar la recuperación

DICCIONARIO DE DATOS

- Atacante: Persona con grandes conocimientos en el manejo de las tecnologías de la información que investiga un sistema informático para reportar fallos de seguridad y desarrollar técnicas que previenen accesos no autorizados.
- Código Arbitrario: Capacidad de un atacante para ejecutar comandos o inyectar código en una aplicación, aprovechando generalmente alguna vulnerabilidad.
- Vulnerabilidad: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina exploit).

REFERENCIAS

1. https://www.cisa.gov/known-exploited-vulnerabilities-cataloghttps://www.fortiguard.com/threat-research/map/country/GT
2. https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-41049
3. https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-410