	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°184	Fecha: 07-08-2023
		Página: 7 de 12

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades en Microsoft Edge		
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 múltiples vulnerabilidades de severidad **ALTA** de tipo desbordamiento de búfer basado en montón, confusión de tipos, escritura fuera de límites, desbordamiento de búfer, usar después de liberar, error de validación de entrada y verificación de seguridad implementada incorrectamente para el estándar en Microsoft Edge. La explotación exitosa de estas vulnerabilidades puede resultar en un compromiso completo del sistema vulnerable y obtenga acceso a información confidencial.

2. DETALLES:

La vulnerabilidad registrada con el código CVE-2023-4068, CVE-2023-4069, CVE-2023-4070 de severidad **crítica** de tipo confusión de tipos existe debido a un error de confusión de tipo dentro del componente V8 en Google Chrome. Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite, desencadenar un error de confusión de tipo y ejecutar código arbitrario en el sistema de destino.

La vulnerabilidad registrada con el código CVE-2023-4071 de severidad **crítica** de tipo desbordamiento de búfer basado en montón, existe debido a un error de límite al procesar contenido HTML que no es de confianza en Visuals. Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la abra, desencadenar un desbordamiento de búfer basado en montón y ejecutar código arbitrario en el sistema de destino.

La vulnerabilidad registrada con el código CVE-2023-4072 de severidad **alta** de tipo escritura fuera de límites, existe debido a un error de límite en WebGL en Google Chrome. Un atacante remoto puede crear un sitio web especialmente diseñado, engañar a la víctima para que lo abra, desencadenar una escritura fuera de los límites y ejecutar código arbitrario en el sistema de destino.

La vulnerabilidad registrada con el código CVE-2023-4073 de severidad **alta** de tipo desbordamiento de búfer, existe debido a un error de límite en ANGLE en Google Chrome. Un atacante remoto puede engañar a la víctima para que visite una página web especialmente diseñada, desencadenar un desbordamiento de búfer basado en pila y ejecutar código arbitrario en el sistema.

La vulnerabilidad registrada con el código CVE-2023-4074 de severidad **alta** de tipo usar después de liberar, existe debido a un error use-after-free dentro del componente Blink Task Scheduling en Google Chrome. Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite, desencadenar un error de uso después de libre y ejecutar código arbitrario en el sistema de destino.

La vulnerabilidad registrada con el código CVE-2023-4075 de severidad **alta** de tipo usar después de liberar, existe debido a un error use-after-free dentro del componente Cast en Google Chrome. Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite, desencadenar un error de uso después de libre y ejecutar código arbitrario en el sistema de destino.

La vulnerabilidad registrada con el código CVE-2023-4076 de severidad **alta** de tipo, usar después de liberar, existe debido a un error use-after-free dentro del componente WebRTC en Google Chrome. Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite, desencadenar un error de uso después de libre y ejecutar código arbitrario en el sistema de destino.

La vulnerabilidad registrada con el código CVE-2023-4077 de severidad **alta** de tipo error de validación de entrada, existe debido a una validación insuficiente de la entrada proporcionada por el usuario en Extensiones en Google Chrome. Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite y obtener acceso a información confidencial.

La vulnerabilidad registrada con el código CVE-2023-4078 de severidad **alta** de tipo verificación de seguridad implementada incorrectamente para el estándar, existe debido a una implementación incorrecta en Extensiones en Google Chrome. Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite y obtener acceso a información confidencial.

A. Productos afectados:

- Microsoft Edge: 79.0.309.71 - 115.0.1901.188.

3. RECOMENDACIONES:

- Actualizar el paquete afectado a la última disponible en el sitio web del proveedor que aborda estas vulnerabilidades.

Fuente de Información:	• hxxps://www.cybersecurity-help.cz/vdb/SB2023080744