	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°233	Fecha: 03-10-2023
		Página: 6 de 12

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidades críticas en productos de Microsoft		
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 dos vulnerabilidades de severidad **CRÍTICA** y **ALTA** de tipo escritura fuera de límites y desbordamiento de búfer de montón en múltiples productos de Microsoft. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto realizar una escritura en memoria fuera de los límites y explotar potencialmente la corrupción del montón a través de una página HTML especialmente diseñada.

2. DETALLES:

La vulnerabilidad de severidad **crítica**, identificada por MITRE como CVE-2023-4863 de desbordamiento de búfer de montón en libwebp en el software de código abierto (OSS) de Google Chrome anterior a 116.0.5845.187 y libwebp 1.3.2, podría permitir a un atacante remoto realizar una escritura en memoria fuera de los límites a través de una página HTML diseñada.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-5217 de desbordamiento de búfer del montón en la codificación vp8 en libvpx en Google Chrome anterior a 117.0.5938.132 y libvpx 1.13.1, podría permitir a un atacante remoto explotar potencialmente la corrupción del montón a través de una página HTML diseñada.

A. Productos afectados:

- Microsoft Edge (basado en Chromium).
- Skype para escritorio, versiones anteriores a 8.105.0.208.
- Webp Image Extensions (publicadas en Windows y actualizadas a través de Microsoft Store), versiones anteriores a 1.0.62681.0.
- Microsoft Teams para Mac, versiones anteriores a 1.6.00.26463.
- Microsoft Teams para escritorio, versiones anteriores a 1.6.00.26474.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software una vez que estén disponibles. Microsoft está trabajando para identificar y abordar estas vulnerabilidades lo antes posible.
- Aplicar las mitigaciones según las instrucciones del proveedor o suspender el uso del producto si las mitigaciones no están disponibles.

Fuente de Información:	• hxxps://msrc.microsoft.com/blog/2023/10/microsofts-response-to-open-source-vulnerabilities-cve-2023-4863-and-cve-2023-5217/ • hxxps://www.cve.org/CVERecord?id=CVE-2023-4863 • hxxps://www.cve.org/CVERecord?id=CVE-2023-5217

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°233**	**Fecha: 03-10-2023**
		Página: 8 de 12

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad en Google Chrome		
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 confusión de tipos en Google Chrome. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino.

2. DETALLES:

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-5346 de tipo confusión de tipos, existe debido a un error de confusión de tipos 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, provocar un error de confusión de tipos y ejecutar código arbitrario en el sistema objetivo.

Esta vulnerabilidad, asigna o inicializa un recurso como un puntero, objeto o variable usando un tipo, pero luego accede a ese recurso usando un tipo que es incompatible con el tipo original.

A. Productos afectados:

- Google Chrome: versión 100.0.4896.60 - 117.0.5938.132.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la versión 117.0.5938.149 disponible que aborda esta vulnerabilidad.

Fuente de Información:	• hxxp://chromereleases.googleblog.com/2023/10/stable-channel-update-for-desktop.html