	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°191	Fecha: 15-08-2023
		Página: 10 de 15

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades 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 han reportado múltiples vulnerabilidades de severidad **ALTA** de tipo verificación de seguridad implementada incorrectamente para el estándar, usar después de liberar, desbordamiento de búfer desbordamiento de búfer basado en montón, confusión de tipos en Google Chrome. La explotación exitosa de estas vulnerabilidades permite que un atacante remoto obtenga acceso a información confidencial, comprometa un sistema vulnerable y ejecute código arbitrario en el sistema de destino.

2. **DETALLES:**

Las vulnerabilidades de severidad **alta** registradas con el código CVE-2023-4359, CVE-2023-4365, CVE-2023-4364, CVE-2023-4363, CVE-2023-4361 y CVE-2023-4360 de tipo verificación de seguridad implementada incorrectamente para el estándar, existen debido a una implementación incorrecta en el Iniciador de aplicaciones, fullscrren, solicitudes, WebShare, Autocompletar y color 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 de severidad **alta** registrada con el código CVE-2023-2312 de tipo usar después de liberar, existe debido a un error use-after-free dentro del componente Offline 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 de severidad **alta** registrada con el código CVE-2023-4355 de tipo desbordamiento de búfer, existe debido a un error de límite en V8 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.

Las vulnerabilidades de severidad **alta** registradas con el código CVE-2023-4354 y CVE-2023-4353 de tipo desbordamiento de búfer basado en montón, existen debido a un error de límite al procesar contenido HTML que no es de confianza en Skia y en ANGLE. 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 de severidad **alta** registrada con el código CVE-2023-4352 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.

Las vulnerabilidades de severidad **alta** registradas con el código CVE-2023-4351 y CVE-2023-4349 de tipo usar después de liberar, existen debido a un error de uso después de liberación dentro del componente Red 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.

Se han asignado los siguientes identificadores para las vulnerabilidades de severidad **media**: CVE-2023-4368, CVE-2023-4367, CVE-2023-4366, CVE-2023-4358, CVE-2023-4357, CVE-2023-4356, CVE-2023-4350 y CVE-2023-4362

A. Productos afectados:

- Google Chrome: 100.0.4896.60 - 115.0.5790.171.

3. **RECOMENDACIÓN:**

- Actualizar el producto afectado a la versión 116.0.5845.96 disponible desde el sitio web del proveedor.

Fuente de Información:	• hxxp://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop_15.html