DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°010**	**Fecha: 11-01-2024**
		Página: 8 de 11

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades críticas en Google ChromeOS TLS		
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 **CRÍTICA** de tipo desbordamiento de enteros, uso después de liberación, control de seguridad implementado incorrectamente para el estándar, y desbordamiento de búfer heap-based en Google ChromeOS TLS. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino, obtener acceso a información confidencial y permitir a un usuario escalar privilegios en el sistema.

2. DETALLES:

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2023-6345 de tipo desbordamiento de enteros, existe debido a un desbordamiento de enteros en el componente Skia de Google Chrome. Un atacante remoto puede engañar a la víctima para que abra una página web especialmente diseñada, provocar un desbordamiento de enteros y ejecutar código arbitrario en el sistema de destino.

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2023-7024 de tipo desbordamiento de búfer heap-based, existe debido a un error de límite al procesar contenido HTML que no es de confianza en WebRTC. Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la abra, provocar un desbordamiento de búfer heap-based y ejecutar código arbitrario en el sistema objetivo.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2023-5851 de tipo control de seguridad implementado incorrectamente para el estándar, existe debido a una implementación incorrecta en Descargas 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 **media,** identificada por MITRE como CVE-2023-5852 de tipo uso después de liberación, existe debido a un error de uso después de la liberación en la impresión en Google Chrome. Un atacante remoto puede engañar a la víctima para que visite una página web especialmente diseñada, provocar un error de uso después de la liberación y obtener acceso a información confidencial.

La vulnerabilidad de severidad **media,** identificada por MITRE como CVE-2023-5855 de tipo uso después de liberación, existe debido a un error de uso después de la liberación en el modo de lectura de Google Chrome. Un atacante remoto puede engañar a la víctima para que visite una página web especialmente diseñada, provocar un error de uso después de la liberación y obtener acceso a información confidencial.

Se ha asignado el siguiente identificador para la vulnerabilidad de severidad baja: CVE-2023-5197.

A. Productos afectados:

- Chrome OS: antes de 114.0.5735.346.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda estas vulnerabilidades.

Fuente de Información:	• hxxp://chromereleases.googleblog.com/2024/01/long-term-support-channel-update-for.html