	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°046	Fecha: 22-02-2024
		Página: 5 de 11

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades 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** y **ALTA** de tipo desbordamiento de enteros, desbordamiento de búfer basado en montón y uso después de la liberación en Google ChromeOS TLS. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino.

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 **alta,** identificada por MITRE como CVE-2024-1283 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 Skia. Un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la abra, provocar un desbordamiento de búfer basado en el montón y ejecutar código arbitrario en el sistema objetivo.

   La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-1284 de tipo uso después de la liberación, existe debido a un error de uso después de la liberación dentro del componente Mojo 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 uso después de la liberación y ejecutar código arbitrario en el sistema de destino.

   A. **Productos afectados:**

      - Chrome OS: anterior a 120.0.6099.294.

3. **RECOMENDACIÓN:**

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

Fuente de Información:	• hxxp://chromereleases.googleblog.com/2024/02/long-term-support-channel-update-for_21.html