	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°232	Fecha: 02-10-2023
		Página: 8 de 13

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades críticas en Google Android		
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 del búfer basado en montón, validación de entrada incorrecta, úselo después de liberarlo, uso de compensación del puntero fuera de rango, autenticación inadecuada, sobrelectura del búfer en Google Android. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar código arbitrario y escalar privilegios en el sistema de destino.

2. **DETALLES:**

Las vulnerabilidades de severidad **crítica**, identificadas por MITRE como CVE-2023-5129 y CVE-2023-4863 de tipo desbordamiento de búfer basado en montón, existe debido a un error de límite al procesar imágenes WebP dentro de la biblioteca libwebp. Un atacante remoto puede engañar a la víctima para que visite un sitio web malicioso, provocar un desbordamiento de búfer basado en el montón y ejecutar código arbitrario en el sistema de destino. La vulnerabilidad afecta a todos los navegadores modernos que admiten el procesamiento de imágenes WebP.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-40129 de tipo validación de entrada incorrecta, existe debido a una validación de entrada incorrecta dentro del componente del sistema. Un atacante remoto puede engañar a la víctima para que abra un archivo especialmente diseñado y ejecute código arbitrario.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-4211 de tipo úselo después de liberarlo, existe debido a un error de uso después de la liberación dentro del controlador del kernel de GPU de Mali. Una aplicación local puede provocar daños en la memoria y ejecutar código arbitrario con privilegios elevados.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-24855 de tipo uso de compensación del puntero fuera de rango, existe debido a una validación de entrada incorrecta en el módem. Un atacante remoto puede ejecutar código arbitrario.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-28540 de tipo autenticación inadecuada, existe debido a una validación de entrada incorrecta en el módem de datos. Un atacante remoto puede leer y manipular datos.

Las vulnerabilidades de severidad **alta**, identificadas por MITRE como CVE-2023-22385, CVE-2023-24848 y CVE-2023-24849 de tipo sobrelectura del búfer, existe debido a una validación de entrada incorrecta en el módem de datos. Un atacante remoto puede leer y manipular datos.

La vulnerabilidad de severidad **alta**, identificada por MITRE como CVE-2023-33028 de tipo desbordamiento del búfer basado en pila, existe debido a una validación de entrada incorrecta en el firmware WLAN. Un atacante remoto puede ejecutar código arbitrario.

A. Productos afectados:

- Google Android: antes del 13 2023-10-05.
- Google Android: antes del 13 2023-10-06.
- Google Android: antes del 13 2023-10-01.

3. **RECOMENDACIONES:**

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

Fuente de Información:	• hxxp://source.android.com/docs/security/bulletin/2023-10-01#2023-10-06-security-patch-level-vulnerability-details • hxxp://source.android.com/docs/security/bulletin/2023-10-01