Actualización de seguridad de Android-Febrero 2024

CYBERZAINTZA- ACTUALIZACIONES-ANDROID-2024-FEBRERO

TLP: CLEAR

www.ciberseguridad.eus

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que la Agencia de Ciberseguridad Vasca considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso la Agencia de Ciberseguridad Vasca puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de la Agencia de Ciberseguridad Vasca como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de la Agencia de Ciberseguridad Vasca. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

1. Resumen ejecutivo

Google ha publicado las actualizaciones de seguridad de **Android** y **dispositivos Píxel** del mes de **febrero de 2024**, en donde se corrigen **53 vulnerabilidades**, que abarcan soluciones para fallos de elevación de privilegios, divulgación de información y ejecución remota de código.

De todas ellas, **46** afectan al sistema operativo **Android,** dentro de las cuales **1** tiene una **severidad crítica** y **45 alta**. En cuanto a los dispositivos **Google Pixel**, se corrigen **7** vulnerabilidades, con **1** de **severidad alta** y **6 moderadas**.

Para prevenir estas y otras vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible.

2. Recursos afectados

Las actualizaciones de seguridad del mes de febrero de 2024 están asociadas a vulnerabilidades que afectan a los siguientes productos:

- Componentes Qualcomm
- Componentes Mediatek
- Componentes Arm
- Componentes Unisoc

3. Análisis técnico

Los detalles de las vulnerabilidades de más relevancia tratadas en esta actualización son los siguientes:

CVE-2024-0031: vulnerabilidad de ejecución remota de código en Android 11, 12, 12L, 13, 14. La vulnerabilidad permanece en estado reservado a fecha de publicación de este informe.

CVE-2023-33072: vulnerabilidad de corrupción de memoria en el core durante el procesamiento de funciones de control.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 120: Buffer Copy Without Checking Size of Input ('Classic Buffer Overflow')

CVSS Base: **9.3**

CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

- **Vector de ataque**: Local
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: **Con cambios**
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2023-43520: vulnerabilidad de corrupción de la memoria cuando AP incluye TID para vincular el IE de mapeo en las balizas y STA está analizando el TID de baliza para vincular el IE de mapeo.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 121: Stack-based Buffer Overflow

CVSS Base: **8.6**

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad:** Baja
- **Integridad:** Baja
- **Disponibilidad: Alta**

CVE-2023-43534: vulnerabilidad de corrupción de la memoria al validar el TID para el marco de solicitud de acción de mapeo de enlaces, cuando una estación se conecta a un punto de acceso.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 823: Use of Out-of-range Pointer Offset

CVSS Base: **8.6**

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad:** Baja
- **Integridad:** Baja
- **Disponibilidad: Alta**

CVE-2023-33058: vulnerabilidad de divulgación de información en Modem durante el procesamiento SIB5.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 126: Buffer Over-read

CVSS Base: **8.2**

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:L

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad:** Ninguna
- **Disponibilidad:** Baja

A continuación, se detalla la lista con todas las vulnerabilidades identificadas:

Framework

CVE	Tipo	Severidad	Versiones
CVE-2024-0029	Elevación de privilegios	Alta	13
CVE-2024-0032	Elevación de privilegios	Alta	11, 12, 12L, 13, 14

CVE-2024-0034	Elevación de privilegios	Alta	11, 12, 12L, 13
CVE-2024-0036	Elevación de privilegios	Alta	11, 12, 12L, 13, 14
CVE-2024-0038	Elevación de privilegios	Alta	14
CVE-2024-0041	Elevación de privilegios	Alta	14
CVE-2023-40122	Divulgación de información	Alta	11, 12, 12L, 13, 14
CVE-2024-0037	Divulgación de información	Alta	11, 12, 12L, 13, 14
CVE-2024-0040	Divulgación de información	Alta	11, 12, 12L, 13, 14

Sistema

CVE	Tipo	Severidad	Versiones
CVE-2024-0031	Ejecución remota de código	**Crítica**	11, 12, 12L, 13, 14
CVE-2024-0014	Elevación de privilegios	Alta	11, 12, 12L, 13, 14
CVE-2024-0033	Elevación de privilegios	Alta	11, 12, 12L, 13, 14
CVE-2024-0035	Elevación de privilegios	Alta	11, 12, 12L, 13, 14
CVE-2023-40093	Divulgación de información	Alta	11, 12, 12L, 13, 14
CVE-2024-0030	Divulgación de información	Alta	11, 12, 12L, 13, 14

Componentes Arm

CVE	Severidad	Subcomponente
CVE-2023-5091	Alta	Mali
CVE-2023-5249	Alta	Mali

CVE-2023-5643	Alta	Mali

Componentes MediaTek

CVE	Severidad	Subcomponente
CVE-2024-20011	Alta	alac decoder
CVE-2024-20006	Alta	DA
CVE-2024-20007	Alta	mp3 decoder
CVE-2024-20009	Alta	alac decoder
CVE-2024-20010	Alta	keyInstall
CVE-2023-32841	Alta	5G Modem
CVE-2023-32842	Alta	5G Modem
CVE-2023-32843	Alta	5G Modem
CVE-2024-20003	Alta	5G Modem

Componentes Unisoc

CVE	Severidad	Subcomponente
CVE-2023-49667	Alta	Kernel
CVE-2023-49668	Alta	Kernel

Componentes Qualcomm

CVE	Severidad	Subcomponente
CVE-2023-43513	Alta	Kernel
CVE-2023-43516	Alta	Video
CVE-2023-43520	Alta	WLAN
CVE-2023-43534	Alta	WLAN

Componentes Qualcomm de código cerrado

CVE	Severidad	Subcomponente
CVE-2023-33046	Alta	Componente de código cerrado
CVE-2023-33049	Alta	Componente de código cerrado
CVE-2023-33057	Alta	Componente de código cerrado
CVE-2023-33058	Alta	Componente de código cerrado

CVE-2023-33060	Alta	Componente de código cerrado
CVE-2023-33072	Alta	Componente de código cerrado
CVE-2023-33076	Alta	Componente de código cerrado
CVE-2023-43518	Alta	Componente de código cerrado
CVE-2023-43519	Alta	Componente de código cerrado
CVE-2023-43522	Alta	Componente de código cerrado
CVE-2023-43523	Alta	Componente de código cerrado
CVE-2023-43533	Alta	Componente de código cerrado
CVE-2023-43536	Alta	Componente de código cerrado

Pixel

CVE	Tipo	Severidad	Subcomponente
CVE-2024-22012	Escalada de privilegios	Alta	Bootloader

Componentes Qualcomm

CVE	Severridad	Subcomponente
CVE-2023-33064	Moderada	Audio
CVE-2023-33065	Moderada	Audio
CVE-2023-33067	Moderada	Audio
CVE-2023-33068	Moderada	Audio
CVE-2023-33069	Moderada	Audio

Componentes Qualcomm de código cerrado

CVE	Severidad	Subcomponente
CVE-2023-33077	Moderada	Componente de código cerrado

4. Mitigación / Solución

Para la mitigación y la corrección de todas las vulnerabilidades, Google publica las actualizaciones de seguridad pertinentes junto a las notas para la mitigación, los cuales están disponibles en los Boletines de Seguridad de Android.

5. Referencias Adicionales

- Boletín de seguridad de Android: febrero de 2024.
- Boletín de actualizaciones de Píxel: febrero de 2024.
- Boletín de seguridad de Qualcomm febrero 2024.
- Mitigaciones de servicios de Android y Google.
- Boletín de seguridad MediaTek febrero 2024.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY