Actualización de seguridad de Android-Abril 2024

CYBERZAINTZA- ACTUALIZACIONES-ANDROID-2024-ABRIL

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 **abril de 2024**, donde se corrigen **53 vulnerabilidades**, que abarcan soluciones para fallos de elevación de privilegios, divulgación de información y denegación de servicio.

De todas ellas, **28** afectan al sistema operativo **Android,** dentro de las cuales **1** tiene una **severidad crítica** y **27 alta**. En cuanto a los dispositivos **Google Pixel**, se corrigen **25** vulnerabilidades, siendo **1** de **severidad crítica, 23 altas** y **1 media.**

De las vulnerabilidades analizadas cabe destacar las identificadas como CVE-2024-29745 y CVE-2024-29748 que afectan a los dispositivos Google Píxel y de las que, según indica Google, **hay indicios de explotación**.

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 abril de 2024 están asociadas a vulnerabilidades que afectan a los siguientes productos:

- Componentes Qualcomm.
- Componentes Mediatek.
- Componentes Widevine.

3. Análisis técnico

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

CVE-2023-28582: vulnerabilidad crítica de corrupción de la memoria en data modem al verificar el mensaje de verificación de saludo durante el proceso de enlace DTLS. Esta vulnerabilidad afecta a un subcomponente de código cerrado de Qualcomm.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **9.8**

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

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

CVE-2024-21468: vulnerabilidad de corrupción de memoria de criticidad alta, cuando falla la operación de desasignación de memoria en la GPU.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **8.4**

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

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

CVE-2024-21472: vulnerabilidad de corrupción de memoria en el kernel mientras maneja operaciones de GPU.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **8.4**

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

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

CVE-2023-28547: vulnerabilidad causada por la corrupción de memoria en la aplicación SPS al solicitar la clave pública en el TA del clasificador.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **8.4**

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

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

CVE-2023-33023: vulnerabilidad causada por la corrupción de memoria al procesar el comando *finish_sign* para pasar un búfer de respuesta (rsp).

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **8.4**

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

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

CVE-2023-32890: En el Módem EMM, existe la posibilidad de un bloqueo del sistema debido a una validación inadecuada de la entrada. Esto podría provocar una denegación de servicio remota sin necesidad de privilegios adicionales de ejecución. No se necesita interacción del usuario para la explotación.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **7.5**

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

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

CVE-2023-33084: vulnerabilidad de denegación de servicio transitoria mientras se procesan fragmentos de IE del servidor durante el handshake DTLS.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **7.5**

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

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

CVE-2023-33086: vulnerabilidad de denegación de servicio transitoria mientras se procesan múltiples solicitudes informativas IKEv2 al dispositivo desde el servidor IPsec con diferentes identificadores.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **7.5**

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

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

CVE-2023-33095: vulnerabilidad de denegación de servicio transitoria al procesar múltiples tipos de contenedores de carga útil con longitud de contenedor incorrecta recibida en la OTA de transporte NAS DL en N.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **7.5**

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

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

CVE-2023-33096: vulnerabilidad de denegación de servicio transitoria durante el procesamiento del mensaje de transporte NAS DL, según lo especificado en el estándar 3GPP 24.501 v16.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **7.5**

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

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

CVE-2023-33099: vulnerabilidad de denegación de servicio transitoria al procesar un contenedor SMS de tamaño no estándar recibido en el transporte NAS DL en NR.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **7.5**

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

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: **Ninguna**

- **Alcance**: Sin cambios
- **Confidencialidad:** Ninguna
- **Integridad:** Ninguna
- **Disponibilidad: Alta**

CVE-2023-33100: vulnerabilidad de denegación de servicio transitoria al procesar un mensaje de transporte NAS DL cuando el ID del mensaje no está definido en la especificación 3GPP.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **7.5**

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

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

CVE-2023-33101: vulnerabilidad de denegación de servicio transitoria al procesar un mensaje de transporte NAS DL con longitud de carga útil 0.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: **7.5**

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

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

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

Framework

CVE	Tipo	Severidad	Versiones
CVE-2024-23710	Elevación de privilegios	Alta	13, 14
CVE-2024-23713	Elevación de privilegios	Alta	12, 12L, 13, 14

CVE-2024-0022	Divulgación de información	Alta	13, 14
CVE-2024-23712	Denegación de servicio	Alta	12, 12L, 13, 14

Sistema

CVE	Tipo	Severidad	Versiones
CVE-2024-23704	Elevación de privilegios	Alta	13, 14
CVE-2023-21267	Divulgación de información	Alta	12, 12L, 13, 14
CVE-2024-0026	Denegación de servicio	Alta	12, 12L, 13, 14
CVE-2024-0027	Denegación de servicio	Alta	12, 12L, 13, 14

Componentes Mediatek

CVE	Severidad	Subcomponente
CVE-2024-20039	Alta	Protocolo de modem
CVE-2024-20040	Alta	Wlan firmware
CVE-2023-32890	Alta	Modem EMM

Widevine

CVE	Severidad	Subcomponente
CVE-2024-0042	Alta	Widevine DRM

Componentes Qualcomm

CVE	Severidad	Subcomponente
CVE-2024-21468	Alta	Kernel
CVE-2024-21472	Alta	Kernel

Componentes Qualcomm de código cerrado

CVE	Severidad	Subcomponente
CVE-2023-28582	**Crítica**	Componente de código cerrado
CVE-2023-28547	Alta	Componente de código cerrado
CVE-2023-33023	Alta	Componente de código cerrado
CVE-2023-33084	Alta	Componente de código cerrado
CVE-2023-33086	Alta	Componente de código cerrado
CVE-2023-33095	Alta	Componente de código cerrado
CVE-2023-33096	Alta	Componente de código cerrado
CVE-2023-33099	Alta	Componente de código cerrado
CVE-2023-33100	Alta	Componente de código cerrado
CVE-2023-33101	Alta	Componente de código cerrado
CVE-2023-33103	Alta	Componente de código cerrado
CVE-2023-33104	Alta	Componente de código cerrado
CVE-2023-33115	Alta	Componente de código cerrado
CVE-2024-21463	Alta	Componente de código cerrado

Pixel

CVE	Tipo	Severidad	Subcomponente
CVE-2024-29740	Elevación de privilegios	**Crítica**	ACPM
CVE-2024-29741	Elevación de privilegios	Alta	S2MPU
CVE-2024-29743	Elevación de privilegios	Alta	ACPM

CVE-2024-29748	Elevación de privilegios	Alta	Pixel Firmware
CVE-2024-29749	Elevación de privilegios	Alta	ACPM
CVE-2024-29752	Elevación de privilegios	Alta	ACPM
CVE-2024-29753	Elevación de privilegios	Alta	ACPM
CVE-2024-29757	Elevación de privilegios	Alta	Companion
CVE-2024-27231	Divulgación de información	Alta	ACPM
CVE-2024-27232	Divulgación de información	Alta	GSC
CVE-2024-29738	Divulgación de información	Alta	ACPM
CVE-2024-29744	Divulgación de información	Alta	ACPM
CVE-2024-29745	Divulgación de información	Alta	Cargador de arranque
CVE-2024-29747	Divulgación de información	Alta	ACPM
CVE-2024-29750	Divulgación de información	Alta	GSC
CVE-2024-29751	Divulgación de información	Alta	GSC
CVE-2024-29754	Divulgación de información	Alta	ACPM
CVE-2024-29755	Divulgación de información	Alta	ACPM
CVE-2024-29782	Divulgación de información	Alta	ACPM
CVE-2024-29783	Divulgación de información	Alta	ACPM
CVE-2024-29746	Elevación de privilegios	Alta	acpm

CVE-2024-29756	Elevación de privilegios	Alta	audio
CVE-2024-29739	Divulgación de información	Alta	ACPM
CVE-2024-29742	Divulgación de información	Alta	ACPM

Componentes Qualcomm

CVE	Severidad	Subcomponente
CVE-2023-43515	Moderada	Cargador de Arranque

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


cyber
zaintza
BASQUE CYBERSECURITY AGENCY