Actualización de seguridad de Android-Marzo 2024

CYBERZAINTZA- ACTUALIZACIONES-ANDROID-2024-MARZO

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 **marzo de 2024**, en donde se corrigen **92 vulnerabilidades**, que abarcan soluciones para fallos de elevación de privilegios, divulgación de información y ejecución remota de código.

De todas ellas, **38** afectan al sistema operativo **Android,** dentro de las cuales **3** tiene una **severidad crítica** y **35 alta**. En cuanto a los dispositivos **Google Pixel**, se corrigen **54** vulnerabilidades, con **16** de **severidad crítica**, **18** de **severidad alta y 20** de **severidad moderada**.

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

- Componentes Qualcomm
- Componentes Mediatek
- Componentes Arm
- Componentes AMLogic

3. Análisis técnico

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

CVE-2023-28578: vulnerabilidad crítica de corrupción de la memoria al ejecutar el comando para eliminar un único detector de eventos que afecta a subcomponente de código cerrado de Qualcomm.

La métrica de evaluación de la vulnerabilidad se compone de:

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-2023-36481: vulnerabilidad crítica de desbordamiento de buffer que afecta a los procesadores móviles y de dispositivos portátiles Samsung Exynos 9810, 9610, 9820, 980, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110 y W920.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 120: Buffer Copy without Checking Size of Input

CVSS Base: **8.6**

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-2024-0039: vulnerabilidad de ejecución remota de código de severidad crítica que afecta a Android 12, 12L, 13, 14. La vulnerabilidad permanece en estado reservado a fecha de publicación de este informe.

CVE-2024-23717: vulnerabilidad crítica de elevación de privilegios en Android 12, 12L, 13, 14. La vulnerabilidad permanece en estado reservado a fecha de publicación de este informe.

CVE-2023-50805: vulnerabilidad de ejecución remota de código de severidad crítica que afecta a pixel, concretamente al subcomponente módem. La vulnerabilidad permanece en estado reservado a fecha de publicación de este informe.

CVE-2023-50807: vulnerabilidad de ejecución remota de código de severidad crítica que afecta a píxel, al subcomponente banda base. La vulnerabilidad permanece en estado reservado a fecha de publicación de este informe.

CVE-2024-27228: vulnerabilidad de ejecución remota de código de severidad crítica que afecta al subcomponente MFC de píxel. La vulnerabilidad permanece en estado reservado a fecha de publicación de este informe.

CVE-2024-22008: vulnerabilidad de escalada de privilegios de severidad crítica que afecta al subcomponente ACPM de píxel. La vulnerabilidad permanece en estado reservado a fecha de publicación de este informe.

CVE-2024-22009: vulnerabilidad de escalada de privilegios de severidad crítica que afecta al subcomponente ACPM de píxel. La vulnerabilidad permanece en estado reservado a fecha de publicación de este informe.

CVE-2024-25986: vulnerabilidad de escalada de privilegios de severidad crítica que afecta al subcomponente LDFW de píxel. La vulnerabilidad permanece en estado reservado a fecha de publicación de este informe.

CVE-2024-27204: vulnerabilidad de escalada de privilegios de severidad crítica que afecta al subcomponente ACPM de píxel. La vulnerabilidad permanece en estado reservado a fecha de publicación de este informe.

CVE-2024-27208: vulnerabilidad de escalada de privilegios de severidad crítica que afecta al subcomponente ACPM de píxel. La vulnerabilidad permanece en estado reservado a fecha de publicación de este informe.

CVE-2024-27210: vulnerabilidad de escalada de privilegios de severidad crítica que afecta al subcomponente ACPM de píxel. La vulnerabilidad permanece en estado reservado a fecha de publicación de este informe.

CVE-2024-27212: vulnerabilidad de escalada de privilegios de severidad crítica que afecta al subcomponente ACPM de píxel. La vulnerabilidad permanece en estado reservado a fecha de publicación de este informe.

CVE-2024-27219: vulnerabilidad de escalada de privilegios de severidad crítica que afecta al subcomponente ACMP de píxel. La vulnerabilidad permanece en estado reservado a fecha de publicación de este informe.

CVE-2024-27220: vulnerabilidad de escalada de privilegios de severidad crítica que afecta al subcomponente ACPM de píxel. La vulnerabilidad permanece en estado reservado a fecha de publicación de este informe.

CVE-2024-27221: vulnerabilidad de escalada de privilegios de severidad crítica que afecta al subcomponente ACPM de píxel. La vulnerabilidad permanece en estado reservado a fecha de publicación de este informe.

CVE-2024-27226: vulnerabilidad de escalada de privilegios de severidad crítica que afecta al subcomponente ACPM de píxel. La vulnerabilidad permanece en estado reservado a fecha de publicación de este informe.

CVE-2024-27233: vulnerabilidad de escalada de privilegios de severidad crítica que afecta al subcomponente LDFW de píxel. La vulnerabilidad permanece en estado reservado a fecha de publicación de este informe.

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

Framework

CVE	Tipo	Severidad	Versiones
CVE-2024-0044	Elevación de privilegios	Alta	12, 12L, 13, 14
CVE-2024-0046	Elevación de privilegios	Alta	12, 12L, 13, 14
CVE-2024-0048	Elevación de privilegios	Alta	12, 12L, 13, 14
CVE-2024-0049	Elevación de privilegios	Alta	12, 12L, 13, 14
CVE-2024-0050	Elevación de privilegios	Alta	12, 12L, 13, 14
CVE-2024-0051	Elevación de privilegios	Alta	12, 12L, 13, 14
CVE-2024-0053	Divulgación de información	Alta	12, 12L, 13, 14
CVE-2024-0047	Denegación de servicio	Alta	14

Sistema

CVE	Tipo	Severidad	Versiones
CVE-2024-0039	Ejecución remota de código	**Crítica**	12, 12L, 13, 14

CVE-2024-23717	Elevación de privilegios	**Crítica**	12, 12L, 13, 14
CVE-2023-40081	Divulgación de información	Alta	12, 12L, 13, 14
CVE-2024-0045	Divulgación de información	Alta	12, 12L, 13, 14
CVE-2024-0052	Divulgación de información	Alta	14

Am Logic

CVE	Severidad	Subcomponente
CVE-2023-48424	Alta	Cargador de arranque
CVE-2023-48425	Alta	Cargador de arranque

Componentes Arm

CVE	Severidad	Subcomponente
CVE-2023-6143	Alta	Mali
CVE-2023-6241	Alta	Mali

Componentes MediaTek

CVE	Severidad	Subcomponente
CVE-2024-20005	Alta	DA
CVE-2024-20022	Alta	LK
CVE-2024-20023	Alta	Flashc
CVE-2024-20024	Alta	Flashc
CVE-2024-20025	Alta	DA
CVE-2024-20027	Alta	DA
CVE-2024-20028	Alta	DA
CVE-2024-20020	Alta	OPTAR
CVE-2024-20026	Alta	DA

Componentes Qualcomm

CVE	Severidad	Subcomponente
CVE-2023-43546	Alta	Security
CVE-2023-43547	Alta	Security
CVE-2023-43550	Alta	Kernel
CVE-2023-43552	Alta	WLAN
CVE-2023-43553	Alta	WLAN

Componentes Qualcomm de código cerrado

CVE	Severidad	Subcomponente
CVE-2023-28578	**Crítica**	Componente de código cerrado
CVE-2023-33042	Alta	Componente de código cerrado
CVE-2023-33066	Alta	Componente de código cerrado
CVE-2023-33105	Alta	Componente de código cerrado
CVE-2023-43539	Alta	Componente de código cerrado
CVE-2023-43548	Alta	Componente de código cerrado
CVE-2023-43549	Alta	Componente de código cerrado

Componentes Kernel

CVE	Tipo	Severidad	Subcomponente
CVE-2024-25987	Escalada de privilegios	Moderada	PT

Pixel

CVE	Tipo	Severidad	Subcomponente
CVE-2023-36481	Ejecución remota de código	**Crítica**	módem
CVE-2023-50805	Ejecución remota de código	**Crítica**	Banda base

CVE-2023-50807	Ejecución remota de código	**Crítica**	Banda base
CVE-2024-27228	Ejecución remota de código	**Crítica**	MFC
CVE-2024-22008	Escalada de privilegios	**Crítica**	ACPM
CVE-2024-22009	Escalada de privilegios	**Crítica**	ACPM
CVE-2024-25986	Escalada de privilegios	**Crítica**	LDFW
CVE-2024-27204	Escalada de privilegios	**Crítica**	ACPM
CVE-2024-27208	Escalada de privilegios	**Crítica**	ACPM
CVE-2024-27210	Escalada de privilegios	**Crítica**	ACPM
CVE-2024-27212	Escalada de privilegios	**Crítica**	ACPM
CVE-2024-27219	Escalada de privilegios	**Crítica**	ACPM
CVE-2024-27220	Escalada de privilegios	**Crítica**	ACPM
CVE-2024-27221	Escalada de privilegios	**Crítica**	ACPM
CVE-2024-27226	Escalada de privilegios	**Crítica**	ACPM
CVE-2024-27233	Escalada de privilegios	**Crítica**	LDFW
CVE-2024-27227	Ejecución remota de código	Alta	Módem
CVE-2023-49927	Escalada de privilegios	Alta	Módem
CVE-2023-50804	Escalada de privilegios	Alta	Módem
CVE-2023-50806	Escalada de privilegios	Alta	Módem

CVE-2024-22005	Escalada de privilegios	Alta	WiFi
CVE-2024-25985	Escalada de privilegios	Alta	gchip
CVE-2024-25992	Escalada de privilegios	Alta	ACPM
CVE-2024-25993	Escalada de privilegios	Alta	ACPM
CVE-2024-27209	Escalada de privilegios	Alta	Módem
CVE-2024-22006	Divulgación de información	Alta	ACPM
CVE-2024-22007	Divulgación de información	Alta	ACPM
CVE-2024-22011	Divulgación de información	Alta	Módem
CVE-2024-25988	Divulgación de información	Alta	Módem de píxeles
CVE-2024-25991	Divulgación de información	Alta	ACPM/TMU
CVE-2024-27218	Divulgación de información	Alta	ACPM
CVE-2024-27234	Divulgación de información	Alta	ACPM
CVE-2024-27235	Divulgación de información	Alta	ACPM
CVE-2024-27229	Denegación de servicio	Alta	GsmSs
CVE-2024-25990	Ejecución remota de código	Moderada	CPIF
CVE-2024-27205	Ejecución remota de código	Moderada	Bluetooth
CVE-2024-27207	Ejecución remota de código	Moderada	Telefonía
CVE-2024-27211	Ejecución remota de código	Moderada	Módem

CVE-2024-27213	Ejecución remota de código	Moderada	rild_exynos
CVE-2024-27222	Ejecución remota de código	Moderada	Ajustes
CVE-2024-27224	Ejecución remota de código	Moderada	pequeño núcleo
CVE-2024-27236	Ejecución remota de código	Moderada	Núcleo
CVE-2024-22010	Divulgación de información	Moderada	ACPM
CVE-2024-25984	Divulgación de información	Moderada	Estado de vertedero
CVE-2024-25989	Divulgación de información	Moderada	controlador de GPU
CVE-2024-27206	Divulgación de información	Moderada	Módem
CVE-2024-27223	Divulgación de información	Moderada	Módem
CVE-2024-27225	Divulgación de información	Moderada	Broadcom bthal
CVE-2024-27230	Divulgación de información	Moderada	Exynos RIL
CVE-2024-27237	Divulgación de información	Moderada	Cargador de arranque
CVE-2023-37368	Denegación de servicio	Moderada	Módem

Componentes Qualcomm

CVE	Severridad	Subcomponente
CVE-2023-33090	Moderada	Audio

Componentes Qualcomm de código cerrado

CVE	Severidad	Subcomponente
CVE-2023-33078	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: marzo de 2024.
- Boletín de actualizaciones de Píxel: marzo de 2024.
- Boletín de seguridad de Qualcomm marzo 2024.
- Boletín de seguridad MediaTek marzo 2024.
- Mitigaciones de servicios de Android y Google.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY