Basque CyberSecurity Centre

Actualización de seguridad de Android-Mayo 2023

BCSC-ACTUALIZACIONES-ANDROID-2023-MAYO

TLP: CLEAR

www.ciberseguridad.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC 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 BCSC 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 BCSC. 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.

Sobre el BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.

El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

FIRST Improving Security Together
TF-CSIRT Trusted Introducer
CSIRT.es

1. Resumen ejecutivo

Google ha publicado las actualizaciones de seguridad para Android del mes de mayo de 2023 en donde se corrigen 45 vulnerabilidades de las versiones 10, 11, 12 y 13 del sistema operativo y componentes asociados, abarcando soluciones para fallos de denegación de servicio, elevación de privilegios, divulgación de información y ejecución remota de código. A ellas se suman 2 vulnerabilidades tratadas para los dispositivos Google Pixel.

De las 45 vulnerabilidades abordadas para Android, 43 tiene severidad alta y 2 moderada. En cuanto a los dispositivos Google Pixel los dos fallos tratados tienen una severidad moderada.

2. Recursos afectados

Las actualizaciones de seguridad del mes de mayo de 2023 están asociadas a vulnerabilidades que afectan a los siguientes productos:

- Componentes Mediatek
- Componentes Imagination Technologies
- Componentes Qualcomm
- Componentes Unisoc
- Componentes Arm
- Componentes del Kernel

3. Análisis técnico

Los detalles de las vulnerabilidades más relevantes corregidas en la actualización de este mes son los siguientes:

CVE-2022-46394: vulnerabilidad en el controlador del núcleo de la GPU de Arm Mali. Un usuario sin privilegios puede realizar operaciones de procesamiento de GPU incorrectas para obtener acceso a la memoria ya liberada. Esto afecta a de Valhall r39p0 a r41p0 y anterior a 42p0 y Avalon r41p0 antes de r42p0.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 8.8

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

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

CVE-2022-46395: vulnerabilidad en el controlador del núcleo de la GPU de Arm Mali. Un usuario sin privilegios puede realizar operaciones de procesamiento de GPU incorrectas para obtener acceso a la memoria ya liberada. Esto afecta a Midgard de r0p0 a r32p0, Bifrost de r0p0 a r41p0 antes de r42p0, Valhall de r19p0 a r41p0 antes de r42p0 y Avalon r41p0 antes de r42p0.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 416: Use After Free

CVSS Base: 8.8

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

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

CVE-2022-46891: vulnerabilidad en el controlador del núcleo de la GPU de Arm Mali, donde existe una condición de Use-After-Free. Un usuario sin privilegios puede realizar operaciones de procesamiento de GPU incorrectas para obtener

acceso a la memoria ya liberada. Esto afecta a Midgard de r13p0 a r32p0, Bifrost de r1p0 a r40p0 y Valhall de r19p0 a r40p0.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 416: Use After Free

CVSS Base: 8.8

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

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

CVE-2023-21665: vulnerabilidad de corrupción de memoria en Gráficos al importar un archivo.

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-2023-21666: vulnerabilidad de corrupción de memoria en gráficos al acceder a un búfer asignado a través del grupo de gráficos.

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-2023-20993: vulnerabilidad en varias funciones de *SnoozeHelper.java*, donde es posible que no se conserve la configuración debido a una excepción no detectada. Esto podría conducir a una escalada local de privilegios sin necesidad de privilegios de ejecución adicionales. La interacción del usuario no es necesaria para la explotación.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 755: Improper Handling of Exceptional Conditions

TTP

- Táctica: Privilege escalation – TA0004
- Técnica: Exploitation for Privilege Escalation -T1404

CVSS Base: 7.8

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

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

CVE-2022-33305: vulnerabilidad que produce una condición DoS transitoria debido a la falta de referencia del puntero NULL en el módem al enviar mensajes no válidos en DCCH.

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-2022-34144: vulnerabilidad que produce una condición DoS transitoria debido a una afirmación alcanzable en el módem durante la programación de decodificación OSI.

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-2022-40504: vulnerabilidad que produce una condición DoS transitoria debido a una afirmación alcanzable en el módem cuando el UE recibió un mensaje de indicación de datos de enlace descendente de la red.

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-2022-40508: vulnerabilidad que produce una condición DoS transitoria debido a una afirmación alcanzable en el módem cuando el UE recibió un mensaje de indicación de datos de enlace descendente de la red.

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	Referencias	Tipo	Severidad	Versiones
CVE-2021-39617	A-175190844	Escalada de privilegios	Alta	11, 12, 12L
CVE-2022-20338	A-171966843	Escalada de privilegios	Alta	11, 12, 12L
CVE-2023-20993	A-261588851	Escalada de privilegios	Alta	11, 12, 12L, 13
CVE-2023-21109	A-261589597	Escalada de privilegios	Alta	11, 12, 12L, 13
CVE-2023-21117	A-263358101	Escalada de privilegios	Alta	13
CVE-2023-20914	A-189942529	Divulgación de información	Alta	11
CVE-2023-21104	A-259938771	Divulgación de información	Alta	12L, 13
CVE-2023-20930	A-250576066	Denegación de servicio	Alta	11, 12, 12L, 13
CVE-2023-21116	A-256202273	Escalada de privilegios	Moderada	11, 12, 12L, 13

Frameworks

CVE	Referencias	Tipo	Severidad	Versiones
CVE-2023-21110	A-258422365	Escalada de privilegios	Alta	11, 12, 12L, 13

Sistema

CVE	Referencias	Tipo	Severidad	Versiones
CVE-2022-20444	A-197296414	Escalada de privilegios	Alta	11, 12
CVE-2023-21107	A-259385017	Escalada de privilegios	Alta	11, 12, 12L, 13

CVE-2023-21112	A-252763983	Divulgación de información	Alta	11, 12, 12L, 13
CVE-2023-21118	A-269014004	Divulgación de información	Alta	11, 12, 12L, 13
CVE-2023-21103	A-259064622	Denegación de servicio	Alta	11, 12, 12L, 13
CVE-2023-21111	A-256819769	Denegación de servicio	Alta	11, 12, 12L, 13

Actualizaciones del sistema Google Play

Subcomponente	CVE
Controlador de permisos	CVE-2021-39617, CVE-2023-20914

Kernel

CVE	Referencias	Tipo	Severidad	Subcomponente
CVE-2023-21102	A-260821414 Upstream kernel [2]	Escalada de privilegios	Alta	EFI
CVE-2023-21106	A-265016072 Upstream kernel	Escalada de privilegios	Alta	GPU

Componentes del Kernel

CVE	Referencias	Tipo	Severidad	Subcomponente
CVE-2023-0266	A-265303544 Upstream kernel	Escalada de privilegios	Moderada	Kernel

Kernel LTS

Referencias	Versión de lanzamiento de Android	Versión de lanzamiento del kernel	Versión de lanzamiento mínima
A-239830686	12	5.1	5.10.136
A-239977583	12	5.4	5.4.210
A-239978386	11	5.4	5.4.210
A-251538603	13	5.1	5.10.136
A-251540658	13	5.15	5.15.72

Componentes Arm

CVE	Referencias	Severidad	Subcomponente
CVE-2022-4639	A-267360595 *	Alta	Mali
CVE-2022-46395	A-267357916 *	Alta	Mali
CVE-2022-46396	A-259984805 *	Alta	Mali
CVE-2022-46891	A-260149319 *	Alta	Mali
CVE-2023-26085	A-261701167 *	Alta	Arm NNAPI Driver

Imagination Technologies

CVE	Referencias	Severidad	Subcomponente
CVE-2021-0877	A-273754094 *	Alta	PowerVR-GPU

Componentes Mediatek

CVE	Referencias	Severidad	Subcomponente
CVE-2023-20694	A-271785766 M-ALPS07733998 *	Alta	preloader
CVE-2023-20695	A-271788841 M-ALPS07734012 *	Alta	preloader
CVE-2023-20696	A-271788842 M-ALPS07856356 *	Alta	preloader
CVE-2023-20699	A-271788844 M-ALPS07696073 *	Alta	adsp
CVE-2023-20697	A-271785768 M-ALPS07589148 *	Alta	keyinstall
CVE-2023-20698	A-271785769 M-ALPS07589144 *	Alta	keyinstall
CVE-2023-20726	A-271785764 M-ALPS07735968 *	Alta	mnld

Componentes Unisoc

CVE	Referencias	Severidad	Subcomponente
CVE-2022-47469	A-273383823 U-2143205 *	Alta	Kernel
CVE-2022-47470	A-273397872 U-2143207 *	Alta	Kernel
CVE-2022-47486	A-273401256 U-2143210 *	Alta	Kernel
CVE-2022-47487	A-273397882 U-2079517 *	Alta	Android
CVE-2022-47488	A-273409059 U-2064944 *	Alta	Kernel

Componentes Qualcomm

CVE	Referencias	Severidad	Subcomponente
CVE-2023-21665	A-271879598 QC-CR#3400722	Alta	Monitor
CVE-2023-21666	A-271879644 QC-CR#3400780	Alta	Monitor

Componentes Qualcomm de código cerrado

CVE	Referencias	Severidad	Subcomponente
CVE-2022-25713	A-258057293 *	Alta	Componente de código cerrado
CVE-2022-33273	A-258057450 *	Alta	Componente de código cerrado
CVE-2022-33305	A-258057367 *	Alta	Componente de código cerrado
CVE-2022-34144	A-258057329 *	Alta	Componente de código cerrado
CVE-2022-40504	A-258057235 *	Alta	Componente de código cerrado
CVE-2022-40508	A-258057197 *	Alta	Componente de código cerrado

Pixel

CVE	Referencias	Tipo	Severidad	Subcomponente
CVE-2023-21119	A-270965644 *	Denegación de servicio	Moderada	Hardware composer service

Componentes Qualcomm

CVE	Referencias	Severidad	Subcomponente
CVE-2022-33281	A-258053342 QC-CR#3053625	Moderada	Cámara

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: mayo de 2023 | Android Open Source Project.
- Recursos y actualizaciones de seguridad | Android Open Source Project.
- Plazos de las actualizaciones de software en teléfonos Google Pixel - Ayuda de Pixel Phone.
- Comunidad oficial Google-Android.
- Boletín de seguridad de Qualcomm mayo 2023.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA