Basque CyberSecurity Centre

Actualización de seguridad de Android-Marzo 2023

BCSC-ACTUALIZACIONES-ANDROID-2023-MARZO

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 marzo de 2023 donde se corrigen 55 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. De las 55 vulnerabilidades tratadas, 4 tienen una severidad crítica, y 51 alta.

2. Recursos afectados

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

- Componentes Mediatek
- Componentes Qualcomm
- Componentes Unisoc

3. Análisis técnico

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

CVE-2022-33256: vulnerabilidad de corrupción de memoria debido a una validación incorrecta del índice de matriz en el procesador de llamadas multimodo.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 9.8

CWE 129: Improper Validation of Array Index

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-2022-33213: vulnerabilidad de corrupción de memoria que afecta al componente Data Modem debido al desbordamiento del búfer mientras se procesa un paquete PPP.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 7.5

CWE 121: Stack-based Buffer Overflow

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

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

CVE-2023-20951: vulnerabilidad de ejecución remota de código sin necesidad de privilegios de ejecución adicionales, además, la interacción del usuario no es necesaria para su explotación.

CVE-2023-20954: vulnerabilidad de ejecución remota de código sin necesidad de privilegios de ejecución adicionales, además, la interacción del usuario no es necesaria para su explotación.

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

Framework

CVE	Referencias	Tipo	Severidad	Versiones Afectadas
CVE-2023-20906	A-221040577	Escalada de privilegios	Alta	11, 12, 12L, 13
CVE-2023-20911	A-242537498	Escalada de privilegios	Alta	11, 12, 12L, 13
CVE-2023-20917	A-242605257	Escalada de privilegios	Alta	11, 12, 12L, 13
CVE-2023-20947	A-237405974	Escalada de privilegios	Alta	12, 12L, 13
CVE-2023-20963	A-220302519	Escalada de privilegios	Alta	11, 12, 12L, 13
CVE-2023-20956	A-240140929	Divulgación de información	Alta	12, 12L, 13
CVE-2023-20958	A-254803162	Divulgación de información	Alta	13
CVE-2023-20964	A-238177121	Denegación de servicio	Alta	12, 12L, 13

Sistema

CVE	Referencias	Tipo	Severidad	Versiones Afectadas
CVE-2023-20951	A-258652631	Ejecución remota de código	**Crítica**	11, 12, 12L, 13
CVE-2023-20954	A-261867748	Ejecución remota de código	**Crítica**	11, 12, 12L, 13
CVE-2023-20926	A-253043058	Escalada de privilegios	Alta	12, 12L, 13
CVE-2023-20931	A-242535997	Escalada de privilegios	Alta	11, 12, 12L, 13
CVE-2023-20936	A-226927612	Escalada de privilegios	Alta	11, 12, 12L, 13

CVE-2023-20953	A-251778420	Escalada de privilegios	Alta	13
CVE-2023-20955	A-258653813	Escalada de privilegios	Alta	11, 12, 12L, 13
CVE-2023-20957	A-258422561	Escalada de privilegios	Alta	11, 12, 12L
CVE-2023-20959	A-249057848	Escalada de privilegios	Alta	13
CVE-2023-20960	A-250589026	Escalada de privilegios	Alta	12L, 13
CVE-2023-20966	A-242299736	Escalada de privilegios	Alta	11, 12, 12L, 13
CVE-2022-4452	A-251802307	Divulgación de información	Alta	13
CVE-2022-20467	A-225880741	Divulgación de información	Alta	11, 12, 12L, 13
CVE-2023-20929	A-234442700	Divulgación de información	Alta	13
CVE-2023-20952	A-186803518	Divulgación de información	Alta	11, 12, 12L, 13
CVE-2023-20962	A-256590210	Divulgación de información	Alta	13
CVE-2022-20499	A-246539931	Denegación de servicio	Alta	12, 12L, 13
CVE-2023-20910	A-245299920	Denegación de servicio	Alta	11, 12, 12L, 13

Actualizaciones del sistema Google Play

Subcomponente	CVE
Media Codecs	CVE-2023-20956
Permission Controller	CVE-2023-20947
Tethering	CVE-2023-20929
WiFi	CVE-2022-20499, CVE-2023-20910

Kernel

CVE	Referencias	Tipo	Severidad	Subcomponente
CVE-2021-33655	A-240019719	EoP	Alta	Frame Buffer

Componentes Mediatek

CVE	Referencias	Severidad	Subcomponente
CVE-2023-20620	A-264149248 M-ALPS07554558	Alta	adsp
CVE-2023-20621	A-264208866 M-ALPS07664755	Alta	tinysys
CVE-2023-20623	A-264209787 M-ALPS07559778	Alta	ion

Componentes Unisoc

CVE	Referencias	Severidad	Subcomponente
CVE-2022-47459	A-264598465 U-2032124	Alta	Kernel
CVE-2022-47461	A-264834026 U-2066617	Alta	system
CVE-2022-47462	A-264834568 U-2066754	Alta	system
CVE-2022-47460	A-264831217 U-2044606	Alta	Kernel

Componentes Qualcomm

CVE	Referencias	Severidad	Subcomponente
CVE-2022-22075	A-193434313	Alta	Monitor
CVE-2022-40537	A-261468700	Alta	Bluetooth

CVE-2022-40540	A-261470730	Alta	Kernel

Componentes Qualcomm de código cerrado

CVE	Referencias	Severidad	Subcomponente
CVE-2022-33213	A-238106224	**Crítica**	Componente de código cerrado
CVE-2022-33256	A-245402790	**Crítica**	Componente de código cerrado
CVE-2022-25655	A-261469326	Alta	Componente de código cerrado
CVE-2022-25694	A-235102547	Alta	Componente de código cerrado
CVE-2022-25705	A-235102507	Alta	Componente de código cerrado
CVE-2022-25709	A-235102420	Alta	Componente de código cerrado
CVE-2022-33242	A-245402503	Alta	Componente de código cerrado
CVE-2022-33244	A-245402728	Alta	Componente de código cerrado
CVE-2022-33250	A-245403450	Alta	Componente de código cerrado
CVE-2022-33254	A-245403473	Alta	Componente de código cerrado
CVE-2022-33272	A-245403311	Alta	Componente de código cerrado
CVE-2022-33278	A-245402730	Alta	Componente de código cerrado
CVE-2022-33309	A-261468683	Alta	Componente de código cerrado
CVE-2022-40515	A-261469638	Alta	Componente de código cerrado
CVE-2022-40527	A-261470448	Alta	Componente de código cerrado
CVE-2022-40530	A-261471028	Alta	Componente de código cerrado
CVE-2022-40531	A-261469091	Alta	Componente de código cerrado
CVE-2022-40535	A-261470732	Alta	Componente de código cerrado

CVE-2022-33309	A-261468683	Alta	Componente de código cerrado
CVE-2022-40515	A-261469638	Alta	Componente de código cerrado
CVE-2022-40527	A-261470448	Alta	Componente de código cerrado
CVE-2022-40530	A-261471028	Alta	Componente de código cerrado
CVE-2022-40531	A-261469091	Alta	Componente de código cerrado
CVE-2022-40535	A-261470732	Alta	Componente de código cerrado

4. Mitigación / Solución

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

5. Referencias Adicionales

- Boletín de seguridad de Android: marzo 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 marzo 2023.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA