Basque CyberSecurity Centre

Actualización de seguridad de Android-Noviembre 2022

BCSC-ACTUALIZACIONES-ANDROID-2022-NOVIEMBRE

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 noviembre de 2022. Se corrigen 43 vulnerabilidades de las versiones 10, 11, 12 y 13 del sistema operativo y componentes asociados, y 5 vulnerabilidades que afectan a los dispositivos móviles Pixel de Google en los modelos que van desde Pixel 4a a Pixel 7, abarcando soluciones para fallos de denegación de servicio, elevación de privilegios y divulgación de información.

De las 43 vulnerabilidades corregidas para Android, 1 tiene severidad crítica y 42 alta. En cuanto a los dispositivos Google Pixel, se han corregido 2 vulnerabilidades de severidad alta, y 3 moderadas.

Se recomienda la rápida aplicación de las actualizaciones para evitar riesgos.

2. Recursos afectados

Las actualizaciones de seguridad del mes de noviembre de 2022 están asociadas a vulnerabilidades que afectan a los siguientes productos:

- Componentes Mediatek
- Componentes Qualcomm
- Componentes Unisoc
- Componentes de Imagination Technologies

3. Análisis técnico

La vulnerabilidad crítica corregida en esta actualización es:

CVE-2021-35122: vulnerabilidad de validación de entrada incorrecta en los chipsets Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, debido a una región no segura que puede intentar modificar los permisos RG de las xPU del espacio IO.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 9.8

CWE: 20 Improper Input Validation

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**

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

Framework

CVE	Referencias	Tipo	Severidad	Versiones Afectadas
CVE-2022-2209	A-235601882	Elevación de privilegios	Alta	10, 11, 12, 12L, 13
CVE-2022-20441	A-238605611	Elevación de privilegios	Alta	10, 11, 12, 12L, 13
CVE-2022-20446	A-229793943	Elevación de privilegios	Alta	10, 11
CVE-2022-20448	A-237540408	Elevación de privilegios	Alta	10, 11, 12, 12L, 13
CVE-2022-20450	A-210065877	Elevación de privilegios	Alta	10, 11, 12, 12L, 13
CVE-2022-20452	A-240138318	Elevación de privilegios	Alta	13
CVE-2022-20457	A-243924784	Elevación de privilegios	Alta	13

Componentes múltiples

CVE	Referencias	Tipo	Severidad	Versiones Afectadas
CVE-2022-20426	A-236263294	Denegación de servicio	Alta	10, 11, 12, 12L, 13

Sistema

CVE	Referencias	Tipo	Severidad	Versiones Afectadas
CVE-2022-20451	A-235098883	Elevación de privilegios	Alta	10, 11, 12, 12L, 13
CVE-2022-20454	A-242096164	Elevación de privilegios	Alta	10, 11, 12, 12L, 13
CVE-2022-20462	A-230356196	Elevación de privilegios	Alta	10, 11, 12, 12L, 13
CVE-2022-20463	A-231985227	Elevación de privilegios	Alta	10, 11, 12, 12L, 13
CVE-2022-20465	A-218500036	Elevación de privilegios	Alta	10, 11, 12, 12L, 13
CVE-2022-20445	A-225876506	Divulgación de información	Alta	10, 11, 12, 12L, 13
CVE-2022-20447	A-233604485	Divulgación de información	Alta	13
CVE-2022-20414	A-234441463	Denegación de servicio	Alta	10, 11, 12, 12L, 13
CVE-2022-20453	A-240685104	Denegación de servicio	Alta	10, 11, 12, 12L, 13

Actualizaciones del sistema Google Play

Subcomponente	CVE
Componentes multimedia del Framework	CVE-2022-2209
WiFi	CVE-2022-20463

Tecnología Imagination

CVE	Referencias	Severidad	Componente
CVE-2021-1050	A-243825200 *	Alta	PowerVR-GPU
CVE-2021-39661	A-246824784 *	Alta	PowerVR-GPU

Componentes Mediatek

CVE	Referencias	Severidad	Subcomponente
CVE-2022-32601	A-234038598 M-ALPS07319132 *	Alta	Telefonía
CVE-2022-32602	A-245050053 M-ALPS07388790 *	Alta	keyinstall

Componentes Unisoc

CVE	Referencias	Severidad	Subcomponentes
CVE-2022-2984	A-244673210 U-1901978 *	Alta	Kernel
CVE-2022-2985	A-244657985 U-1882490 *	Alta	Android
CVE-2022-38669	A-244666286 U-1883755 *	Alta	Android
CVE-2022-38670	A-244674480 U-1883755 *	Alta	Android
CVE-2022-39105	A-245210875 U-1830881 *	Alta	Kernel
CVE-2022-38672	A-244684957 U-1957128 *	Alta	Kernel
CVE-2022-38673	A-246482122 U-1957128 *	Alta	Kernel
CVE-2022-38676	A-244683429 U-1908118 *	Alta	Kernel
CVE-2022-38690	A-244109033 U-1914157 *	Alta	Kernel

Componentes Qualcomm

CVE	Referencias	Severidad	Componentes
CVE-2022-25724	A-238106223 QC-CR#3090325 [2] [3]	Alta	Monitor
CVE-2022-25741	A-240972788 QC-CR#3147273	Alta	WLAN
CVE-2022-25743	A-240973083 QC-CR#3153406	Alta	Monitor

Componentes Qualcomm de código cerrado

CVE	Referencias	Severidad	Subcomponentes
CVE-2021-35122	A-213239915 *	**Crítica**	Componente de código cerrado

CVE-2021-35108	A-209469945 *	Alta	Componente de código cerrado
CVE-2021-35109	A-209469824 *	Alta	Componente de código cerrado
CVE-2021-35132	A-213240063 *	Alta	Componente de código cerrado
CVE-2021-35135	A-213239949 *	Alta	Componente de código cerrado
CVE-2022-25671	A-231156429 *	Alta	Componente de código cerrado
CVE-2022-33234	A-240971780 *	Alta	Componente de código cerrado
CVE-2022-33236	A-240973180 *	Alta	Componente de código cerrado
CVE-2022-33237	A-240972236 *	Alta	Componente de código cerrado
CVE-2022-33239	A-240982982 *	Alta	Componente de código cerrado

Dispositivos Google Pixel

Píxel

CVE	Referencias	Tipo	Severidad	Componente
CVE-2022-20459	A-239556260 *	Elevación de privilegios	Alta	Titan M
CVE-2022-20460	A-239557547 *	Elevación de privilegios	Alta	Titan M

Componentes Qualcomm de código cerrado

CVE	Referencia	Severidad	Subcomponente
CVE-2022-25674	A-231226928 *	Moderada	Componente de código cerrado
CVE-2022-25676	A-231226556 *	Moderada	Componente de código cerrado
CVE-2022-25679	A-215246183 *	Moderada	Componente de código cerrado

4. Mitigación / Solución

Para la mitigación y el parcheo 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: noviembre de 2022 | 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
- Security Bulletins | Qualcomm Documentation

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA