Actualizaciones de seguridad de Android - mayo 2022

BCSC-ACTUALIZACIONES-ANDROID-2022-MAYO

TLP:WHITE

www.basquecybersecurity.eus

Mayo 2022

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:

1. RESUMEN EJECUTIVO

Google ha publicado las actualizaciones de seguridad de Android del mes de mayo de 2022. Se corrigen 37 vulnerabilidades de las versiones 10, 11 y 12 del sistema operativo, y componentes asociados, y 11 vulnerabilidades que afectan a los dispositivos móviles Pixel de Google en los modelos que van desde Pixel 3 a Pixel 6.

De las 37 vulnerabilidades corregidas para Android, 1 tiene una severidad crítica, 2 moderadas y el resto alta. En cuanto a los Google Pixel, se corrigen 11 vulnerabilidades, con 2 de ellas críticas, 4 de severidad alta y 5 moderadas.

Se recomienda la instalación de las correspondientes actualizaciones para corregir los fallos.

2. RECURSOS AFECTADOS

Las actualizaciones de seguridad de Android del mes de mayo de 2022 están asociados a vulnerabilidades que afectan a los siguientes sistemas:

- Google Play.
- Componentes del Kernel.
- Componentes Mediatek.
- Componentes Qualcomm.

3. ANÁLISIS TÉCNICO

De las vulnerabilidades corregidas, las más relevantes son, por una parte, la crítica que afecta a componentes de los procesadores Qualcomm, integrados en algunos dispositivos de los diferentes fabricantes que usan el sistema operativo de Google, y para las que no se ha ofrecido información adicional, con el identificador CVE-2021-35090.

Por otra, las 2 críticas que afectan a los dispositivos Pixel, con los identificadores CVE-2022-20120, que atañe al bootloader, la herramienta que carga el software del sistema operativo y se encarga de realizar las pruebas de comprobación antes de iniciarlo, suministrando las instrucciones para que el dispositivo pueda arrancar sin inconvenientes, y la vulnerabilidad con el identificador **CVE-2022-20117**, que concierne al chip Titan M que se utiliza en los dispositivos Pixel 3 como chip de seguridad, diseñado por la propia Google, y que se encarga de proteger los datos almacenados en los dispositivos, sumando una capa de seguridad extra a la pantalla de bloqueo, y reforzando el cifrado del disco.

Por último, destacar que la vulnerabilidad conocida como Dirty Pipe, de elevación de privilegios, con el identificador CVE-2022-0847, sigue apareciendo listada, tras la actualización de seguridad del mes pasado, esta vez bajo el nivel de la actualización más reciente ofrecida por Google.

A continuación, se detalla la lista de todas las vulnerabilidades corregidas asociadas al sistema afectado:

Framework

CVE	Tipo	Severidad	Versiones
CVE-2021-39662	Elevación de privilegios	Alta	11, 12
CVE-2022-20004	Elevación de privilegios	Alta	10, 11, 12, 12L
CVE-2022-20005	Elevación de privilegios	Alta	10, 11, 12, 12L
CVE-2022-20007	Elevación de privilegios	Alta	10, 11, 12, 12L
CVE-2021-39700	Divulgación de información	Moderada	10, 11, 12

Sistema

CVE	Tipo	Severidad	Versiones
CVE-2022-20113	Elevación de privilegios	Alta	12, 12L
CVE-2022-20114	Elevación de privilegios	Alta	10, 11, 12, 12L
CVE-2022-20116	Elevación de privilegios	Alta	12, 12L
CVE-2022-20010	Divulgación de información	Alta	12, 12L
CVE-2022-20011	Divulgación de información	Alta	10, 11, 12, 12L
CVE-2022-20115	Divulgación de información	Alta	12, 12L
CVE-2021-39670	Denegación de servicio	Alta	12, 12L
CVE-2022-20112	Denegación de servicio	Alta	10, 11, 12, 12L

Actualizaciones del sistema Google Play

CVE	Componente
CVE-2021-39662	Proveedor de medios

Componentes del Kernel

CVE	Tipo	Severidad	Componente
CVE-2022-0847	Elevación de privilegios	Alta	pipes
CVE-2022-20009	Elevación de privilegios	Alta	Linux
CVE-2022-20008	Divulgación de información	Alta	SD MMC
CVE-2021-22600	Elevación de privilegios	Moderada	Kernel

Componentes MediaTek

CVE	Severidad	Componente
CVE-2022-20084	Alta	Telefonía
CVE-2022-20109	Alta	ion
CVE-2022-20110	Alta	ion

Componentes Qualcomm

CVE	Severidad	Componente
CVE-2022-22057	Alta	Monitor
CVE-2022-22064	Alta	Wifi
CVE-2022-22065	Alta	Wifi
CVE-2022-22068	Alta	Kernel
CVE-2022-22072	Alta	Wifi

Componentes de código cerrado Qualcomm

CVE	Severidad	Componente
CVE-2021-35090	**Crítica**	Componente de código cerrado
CVE-2021-35072	Alta	Componente de código cerrado
CVE-2021-35073	Alta	Componente de código cerrado
CVE-2021-35076	Alta	Componente de código cerrado
CVE-2021-35078	Alta	Componente de código cerrado
CVE-2021-35080	Alta	Componente de código cerrado
CVE-2021-35086	Alta	Componente de código cerrado
CVE-2021-35087	Alta	Componente de código cerrado
CVE-2021-35094	Alta	Componente de código cerrado
CVE-2021-35096	Alta	Componente de código cerrado
CVE-2021-35116	Alta	Componente de código cerrado

Dispositivos Google Pixel

CVE	Tipo	Severidad	Componente
CVE-2022-20120	Ejecución remota de código	**Crítica**	Bootloader (cargador de arranque de s.o)
CVE-2022-20117	Divulgación de información	**Crítica**	Titan-M
CVE-2021-4083	Elevación de privilegios	Alta	Kernel
CVE-2022-20118	Elevación de privilegios	Alta	Kernel
CVE-2022-20119	Divulgación de información	Alta	Pantalla/Gráficos
CVE-2022-20121	Divulgación de información	Alta	USCCDMService

Componentes Qualcomm

CVE	Severidad	Componente
CVE-2021-35084	Moderada	Wifi
CVE-2021-35085	Moderada	Wifi
CVE-2021-35092	Moderada	Modem
CVE-2021-35098	Moderada	Audio

Componentes de código cerrado Qualcomm

CVE	Severidad	Componente
CVE-2021-35079	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: mayo 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

Reportar incidente

Si has detectado algún incidente de ciberseguridad, avísanos para que tomemos las medidas oportunas para evitar su propagación.

900 104 891

incidencias@bcsc.eus

Catálogo de ciberseguridad

¿Necesitas ayuda con tu ciberseguridad o la de tu empresa?