Basque CyberSecurity Centre

Actualización de seguridad de Android-Diciembre 2022

BCSC-ACTUALIZACIONES-ANDROID-2022-DICIEMBRE

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 diciembre de 2022. Se corrigen 77 vulnerabilidades de las versiones 10, 11, 12 y 13 del sistema operativo y componentes asociados, y 151 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, divulgación de información y ejecución remota de código.

De las 77 vulnerabilidades corregidas para Android, 4 tiene severidad crítica, 71 alta y 2 moderadas. En cuanto a los dispositivos Google Pixel, se han corregido 16 vulnerabilidades de severidad crítica, 15 de severidad alta, 119 moderadas y 1 baja.

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

2. Recursos afectados

Las actualizaciones de seguridad del mes de diciembre 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

Las vulnerabilidades críticas corregidas, de las que no se dispone de sus métricas de evaluación a fecha de la publicación de este informe, ya que permanecen catalogadas como reservadas por CVE a la espera de información más detallada, son:

CVE-2022-20472: vulnerabilidad de ejecución remota de código en el Framework de Android, que afecta a las versiones que van de la 10 a la 13.

CVE-2022-20473: vulnerabilidad de ejecución remota de código en el Framework de Android, que afecta a las versiones que van de la 10 a la 13.

CVE-2022-20411: vulnerabilidad de ejecución remota de código en el Framework de Android, que afecta a las versiones que van de la 10 a la 13.

CVE-2022-20498: vulnerabilidad de divulgación de información en el sistema de Android, que afecta las versiones que van de la 10 a la 13.

CVE-2022-20582: vulnerabilidad de elevación de privilegios que afecta al componente LDFW.

CVE-2022-20583: vulnerabilidad de elevación de privilegios que afecta al componente LDFW.

CVE-2022-20584: vulnerabilidad de elevación de privilegios que afecta al componente TF-A.

CVE-2022-20585: vulnerabilidad de elevación de privilegios que afecta al componente LDFW.

CVE-2022-20586: vulnerabilidad de elevación de privilegios que afecta al componente LDFW.

CVE-2022-20587: vulnerabilidad de elevación de privilegios que afecta al componente LDFW.

CVE-2022-20588: vulnerabilidad de elevación de privilegios que afecta al componente LDFW.

CVE-2022-20597: vulnerabilidad de elevación de privilegios que afecta al componente LDFW.

CVE-2022-20598: vulnerabilidad de elevación de privilegios que afecta al componente LDFW.

CVE-2022-20599: vulnerabilidad de elevación de privilegios que afecta al firmware de los dispositivos Pixel.

CVE-2022-42534: vulnerabilidad de elevación de privilegios que afecta al componente TF-A.

CVE-2022-20498: vulnerabilidad de elevación de privilegios que afecta al componente libfdt.

CVE-2022-20589: vulnerabilidad de elevación de privilegios que afecta al componente LDFW.

CVE-2022-20590: vulnerabilidad de elevación de privilegios que afecta al componente LDFW.

CVE-2022-20591: vulnerabilidad de elevación de privilegios que afecta al componente LDFW.

CVE-2022-20592: vulnerabilidad de elevación de privilegios que afecta al componente LDFW.

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

Android Runtime

CVE	Referencias	Tipo	Severidad	Versiones Afectadas
CVE-2022-20502	A-222166527	Divulgación de información	Alta	13

Framework

CVE	Referencias	Tipo	Severidad	Versiones Afectadas
CVE-2022-20472	A-239210579	Ejecución remota de código	**Crítica**	10, 11, 12, 12L, 13
CVE-2022-20473	A-239267173	Ejecución remota de código	**Crítica**	10, 11, 12, 12L, 13
CVE-2021-39617	A-175190844	Elevación de privilegios	Alta	11, 12, 12L
CVE-2021-39795	A-201667614	Elevación de privilegios	Alta	11, 12, 12L, 13
CVE-2022-20124	A-170646036	Elevación de privilegios	Alta	10, 11, 12, 12L, 13

CVE-2022-20442	A-176094367	Elevación de privilegios	Alta	10, 11, 12, 12L
CVE-2022-20444	A-197296414	Elevación de privilegios	Alta	11, 12
CVE-2022-20470	A-234013191	Elevación de privilegios	Alta	10, 11, 12, 12L, 13
CVE-2022-20474	A-240138294	Elevación de privilegios	Alta	10, 11, 12, 12L, 13
CVE-2022-20475	A-240663194	Elevación de privilegios	Alta	11, 12, 12L, 13
CVE-2022-20477	A-241611867	Elevación de privilegios	Alta	13
CVE-2022-20485	A-242702935	Elevación de privilegios	Alta	10, 11, 12, 12L, 13
CVE-2022-20486	A-242703118	Elevación de privilegios	Alta	10, 11, 12, 12L, 13
CVE-2022-20491	A-242703556	Elevación de privilegios	Alta	10, 11, 12, 12L, 13
CVE-2022-20611	A-242996180	Elevación de privilegios	Alta	10, 11, 12, 12L, 13
CVE-2021-0934	A-169762606	Denegación de servicio	Alta	10, 11, 12, 12L, 13
CVE-2022-20449	A-239701237	Denegación de servicio	Alta	10, 11, 12, 12L, 13
CVE-2022-20476	A-240936919	Denegación de servicio	Alta	10, 11, 12, 12L
CVE-2022-20482	A-240422263	Denegación de servicio	Alta	12, 12L, 13
CVE-2022-20500	A-246540168	Denegación de servicio	Alta	10, 11, 12, 12L, 13

Media Framework

CVE	Referencias	Tipo	Severidad	Versiones Afectadas
CVE-2022-20496	A-245242273	Divulgación de información	Alta	12, 12L, 13

Sistema

CVE	Referencias	Tipo	Severidad	Versiones Afectadas
CVE-2022-20411	A-232023771	Ejecución remota de código	**Crítica**	10, 11, 12, 12L, 13

CVE-2022-20498	A-246465319	Divulgación de información	**Crítica**	10, 11, 12, 12L, 13
CVE-2022-20469	A-230867224	Ejecución remota de código	Alta	10, 11, 12, 12L, 13
CVE-2022-20144	A-187702830	Elevación de privilegios	Alta	10, 11, 12, 12L, 13
CVE-2022-20240	A-231496105	Elevación de privilegios	Alta	12, 12L
CVE-2022-20478	A-241764135	Elevación de privilegios	Alta	10, 11, 12, 12L, 13
CVE-2022-20479	A-241764340	Elevación de privilegios	Alta	10, 11, 12, 12L, 13
CVE-2022-20480	A-241764350	Elevación de privilegios	Alta	10, 11, 12, 12L, 13
CVE-2022-20484	A-242702851	Elevación de privilegios	Alta	10, 11, 12, 12L, 13
CVE-2022-20487	A-242703202	Elevación de privilegios	Alta	10, 11, 12, 12L, 13
CVE-2022-20488	A-242703217	Elevación de privilegios	Alta	10, 11, 12, 12L, 13
CVE-2022-20495	A-243849844	Elevación de privilegios	Alta	10, 11, 12, 12L, 13
CVE-2022-20501	A-246933359	Elevación de privilegios	Alta	10, 11, 12, 12L, 13
CVE-2022-20466	A-179725730	Divulgación de información	Moderada	13
CVE-2022-20466	A-179725730	Divulgación de información	Alta	10, 11, 12, 12L
CVE-2022-20471	A-238177877	Divulgación de información	Alta	11, 12, 12L, 13
CVE-2022-20483	A-242459126	Divulgación de información	Alta	10, 11, 12, 12L, 13
CVE-2022-20497	A-246301979	Divulgación de información	Alta	12, 12L, 13
CVE-2022-20499	A-246539931	Denegación de servicio	Alta	12, 12L, 13
CVE-2022-20468	A-228450451	Divulgación de información	Moderada	10, 11, 12, 12L, 13

Actualizaciones del sistema Google Play

Subcomponente	CVE
MediaProvider	CVE-2021-39795
Permission Controller	CVE-2021-39617, CVE-2022-20442
WiFi	CVE-2022-20499

Kernel

CVE	Referencias	Tipo	Severidad	Subcomponente
CVE-2022-23960	A-215557547 Upstream kernel [2] [3] [4] [5] [6] [7] [8] [9] [10] [11] [12] [13] [14] [15] [16] [17] [18] [19] [20] [21] [22] [23] [24] [25] [26]	Divulgación de información	Alta	Kernel

Tecnología Imagination

CVE	Referencias	Severidad	Subcomponente
CVE-2021-39660	A-254742984 *	Alta	PowerVR-GPU

Componentes Mediatek

CVE	Referencias	Severidad	Subcomponente
CVE-2022-32594	A-250331397 M-ALPS07446207 *	Alta	widevine
CVE-2022-32596	A-250470698 M-ALPS07446213 *	Alta	widevine
CVE-2022-32597	A-250470696 M-ALPS07446228 *	Alta	widevine
CVE-2022-32598	A-250470697 M-	Alta	widevine

	ALPS07446228 *		
CVE-2022-32619	A-250441021 M-ALPS07439659 *	Alta	keyinstall
CVE-2022-32620	A-250441023 M-ALPS07541753 *	Alta	mpu

Componentes Unisoc

CVE	Referencias	Severidad	Subcomponente
CVE-2022-39106	A-252398972 U-1830881 *	Alta	Kernel
CVE-2022-39131	A-252950986 U-1914157 *	Alta	Kernel
CVE-2022-39132	A-252951342 U-1914157 *	Alta	Kernel
CVE-2022-39133	A-253957345 U-1946077 *	Alta	Kernel
CVE-2022-39134	A-253333208 U-1947682 *	Alta	Kernel
CVE-2022-42754	A-253344080 U-1967614 *	Alta	Kernel
CVE-2022-42755	A-253957344 U-1981296 *	Alta	Kernel
CVE-2022-42756	A-253337348 U-1967535 *	Alta	Kernel
CVE-2022-42770	A-253978051 U-1975103 *	Alta	Kernel
CVE-2022-42771	A-253978040 U-1946329 *	Alta	Kenel
CVE-2022-42772	A-253978054 U-1903041 *	Alta	kernel
CVE-2022-39129	A-252943954 U-1957128 *	Alta	Kernel
CVE-2022-39130	A-252950982 U-1957128 *	Alta	Kernel

Componentes Qualcomm

CVE	Referencias	Severidad	Subcomponente
CVE-2022-33268	A-245992426 QC-	Alta	Bluetooth

	CR#3182085 [2]		

Componentes Qualcomm de código cerrado

CVE	Referencias	Severidad	Subcomponente
CVE-2022-25672	A-231156083 *	Alta	Componente de código cerrado
CVE-2022-25673	A-235102693 *	Alta	Componente de código cerrado
CVE-2022-25681	A-238106628 *	Alta	Componente de código cerrado
CVE-2022-25682	A-238102293 *	Alta	Componente de código cerrado
CVE-2022-25685	A-235102504 *	Alta	Componente de código cerrado
CVE-2022-25689	A-235102546 *	Alta	Componente de código cerrado
CVE-2022-25691	A-235102879 *	Alta	Componente de código cerrado
CVE-2022-25692	A-235102506 *	Alta	Componente de código cerrado
CVE-2022-25695	A-235102757 *	Alta	Componente de código cerrado
CVE-2022-25697	A-235102692 *	Alta	Componente de código cerrado
CVE-2022-25698	A-235102566 *	Alta	Componente de código cerrado
CVE-2022-25702	A-235102898 *	Alta	Componente de código cerrado
CVE-2022-33235	A-245402984 *	Alta	Componente de código cerrado
CVE-2022-33238	A-245402341 *	Alta	Componente de código cerrado

Dispositivos Google Pixel

Framework

CVE	Referencias	Tipo	Severidad	Versiones Afectadas
CVE-2022-20504	A-225878553	Elevación de privilegios	Moderada	13
CVE-2022-20512	A-238602879	Elevación de privilegios	Moderada	13

CVE-2022-20514	A-245727875	Elevación de privilegios	Moderada	13
CVE-2022-20524	A-228523213	Elevación de privilegios	Moderada	13
CVE-2022-20553	A-244155265	Elevación de privilegios	Moderada	13
CVE-2022-20554	A-245770596	Elevación de privilegios	Moderada	13
CVE-2022-20510	A-235822336	Divulgación de información	Moderada	13
CVE-2022-20511	A-235821829	Divulgación de información	Moderada	13
CVE-2022-20513	A-244569759	Divulgación de información	Moderada	13
CVE-2022-20523	A-228222508	Divulgación de información	Moderada	13
CVE-2022-20530	A-231585645	Divulgación de información	Moderada	13
CVE-2022-20538	A-235601770	Divulgación de información	Moderada	13
CVE-2022-20559	A-219739967	Divulgación de información	Moderada	13
CVE-2022-20543	A-238178261	DoS	Moderada	13
CVE-2022-20526	A-229742774	Elevación de privilegios	Baja	13

Media Framework

CVE	Referencias	Tipo	Severidad	Versiones Afectadas
CVE-2022-20548	A-240919398	Elevación de privilegios	Moderada	13
CVE-2022-20528	A-230172711	Divulgación de información	Moderada	13

Sistema

CVE	Referencias	Tipo	Severidad	Versiones Afectadas
CVE-2021-39771	A-224545390	Elevación de privilegios	Moderada	13
CVE-2022-20503	A-224772890	Elevación de privilegios	Moderada	13
CVE-2022-20505	A-225981754	Elevación de privilegios	Moderada	13
CVE-2022-20506	A-226133034	Elevación de privilegios	Moderada	13
CVE-2022-20507	A-246649179	Elevación de privilegios	Moderada	13
CVE-2022-20508	A-218679614	Elevación de privilegios	Moderada	13
CVE-2022-20509	A-244713317	Elevación de privilegios	Moderada	13
CVE-2022-20519	A-224772678	Elevación de privilegios	Moderada	13
CVE-2022-20520	A-227203202	Elevación de privilegios	Moderada	13
CVE-2022-20522	A-227470877	Elevación de privilegios	Moderada	13
CVE-2022-20525	A-229742768	Elevación de privilegios	Moderada	13
CVE-2022-20529	A-231583603	Elevación de privilegios	Moderada	13
CVE-2022-20533	A-232798363	Elevación de privilegios	Moderada	13
CVE-2022-20536	A-235100180	Elevación de privilegios	Moderada	13
CVE-2022-20537	A-235601169	Elevación de privilegios	Moderada	13
CVE-2022-20539	A-237291425	Elevación de privilegios	Moderada	13
CVE-2022-20540	A-237291506	Elevación de privilegios	Moderada	13
CVE-2022-20544	A-238745070	Elevación de privilegios	Moderada	13
CVE-2022-20546	A-240266798	Elevación de privilegios	Moderada	13
CVE-2022-20547	A-240301753	Elevación de privilegios	Moderada	13
CVE-2022-20549	A-242702451	Elevación de privilegios	Moderada	13

CVE-2022-20550	A-242845514	Elevación de privilegios	Moderada	13
CVE-2022-20556	A-246301667	Elevación de privilegios	Moderada	13
CVE-2022-20557	A-247092734	Elevación de privilegios	Moderada	13
CVE-2022-20558	A-236264289	Elevación de privilegios	Moderada	13
CVE-2022-42542	A-231445184	Elevación de privilegios	Moderada	13
CVE-2022-20199	A-199291025	Divulgación de información	Moderada	13
CVE-2022-20515	A-220733496	Divulgación de información	Moderada	13
CVE-2022-20516	A-224002331	Divulgación de información	Moderada	13
CVE-2022-20517	A-224769956	Divulgación de información	Moderada	13
CVE-2022-20518	A-224770203	Divulgación de información	Moderada	13
CVE-2022-20527	A-229994861	Divulgación de información	Moderada	13
CVE-2022-20531	A-231988638	Divulgación de información	Moderada	13
CVE-2022-20535	A-233605242	Divulgación de información	Moderada	13
CVE-2022-20541	A-238083126	Divulgación de información	Moderada	13
CVE-2022-20552	A-243922806	Divulgación de información	Moderada	13
CVE-2022-20555	A-246194233	Divulgación de información	Moderada	13
CVE-2022-42535	A-224770183	Divulgación de información	Moderada	13

CVE-2022-20521	A-227203684	Denegación de servicio	Moderada	13
CVE-2022-20545	A-239368697	Denegación de servicio	Moderada	13

Componentes del Kernel

CVE	Referencias	Tipo	Severidad	Subcomponente
CVE-2022-0500	A-228560539 Upstream kernel	Elevación de privilegios	Moderada	Kernel
CVE-2022-1116	A-234020136 Upstream kernel	Elevación de privilegios	Moderada	Kernel
CVE-2022-1419	A-235540888 Upstream kernel	Elevación de privilegios	Moderada	Kernel
CVE-2022-20565	A-160818461 Upstream kernel	Elevación de privilegios	Moderada	Kernel
CVE-2022-20566	A-165329981 Upstream kernel [2]	Elevación de privilegios	Moderada	Bluetooth L2CAP
CVE-2022-20567	A-186777253 Upstream kernel	Elevación de privilegios	Moderada	Kernel
CVE-2022-20568	A-220738351 Upstream kernel	Elevación de privilegios	Moderada	io_uring
CVE-2022-20571	A-234030265 Upstream kernel	Elevación de privilegios	Moderada	dm-verity
CVE-2022-20572	A-234475629 Upstream kernel [2]	Elevación de privilegios	Moderada	dm-verity
CVE-2022-28390	A-228694391 Upstream kernel	Elevación de privilegios	Moderada	Kernel
CVE-2022-30594	A-233438137 Upstream kernel [2] [3]	Elevación de privilegios	Moderada	Kernel
CVE-2022-34494	A-238479990 Upstream kernel	Elevación de privilegios	Moderada	Kernel

CVE-2022-34495	A-238480163 Upstream kernel	Elevación de privilegios	Moderada	Kernel
CVE-2022-20573	A-235183128 Upstream kernel [2]	Divulgación de información	Moderada	Kernel

Píxel

CVE	Referencias	Tipo	Severidad	Subcomponente
CVE-2022-20582	A-233645166 *	Elevación de privilegios	**Crítica**	LDFW
CVE-2022-20583	A-234859169 *	Elevación de privilegios	**Crítica**	LDFW
CVE-2022-20584	A-238366009 *	Elevación de privilegios	**Crítica**	TF-A
CVE-2022-20585	A-238716781 *	Elevación de privilegios	**Crítica**	LDFW
CVE-2022-20586	A-238718854 *	Elevación de privilegios	**Crítica**	LDFW
CVE-2022-20587	A-238720411 *	Elevación de privilegios	**Crítica**	LDFW
CVE-2022-20588	A-238785915 *	Elevación de privilegios	**Crítica**	LDFW
CVE-2022-20597	A-243480506 *	Elevación de privilegios	**Crítica**	LDFW
CVE-2022-20598	A-242357514 *	Elevación de privilegios	**Crítica**	LDFW
CVE-2022-20599	A-242332706 *	Elevación de privilegios	**Crítica**	Pixel firmware
CVE-2022-42534	A-237838301 *	Elevación de privilegios	**Crítica**	TF-A
CVE-2022-20498	A-249998113 *	Divulgación de información	**Crítica**	libfdt
CVE-2022-20589	A-238841928 *	Divulgación de información	**Crítica**	LDFW
CVE-2022-20590	A-238932493 *	Divulgación de información	**Crítica**	LDFW
CVE-2022-20591	A-238939706 *	Divulgación de información	**Crítica**	LDFW

CVE-2022-20592	A-238976908 *	Divulgación de información	**Crítica**	LDFW
CVE-2022-20603	A-219265339 *	RCE	Alta	Modem
CVE-2022-20607	A-238914868 *	Ejecución remota de código	Alta	Cellular Firmware
CVE-2022-20610	A-240462530 *	Ejecución remota de código	Alta	Pixel cellular modem
CVE-2022-20561	A-222162870 *	Elevación de privilegios	Alta	Audio
CVE-2022-20564	A-243798789 *	Elevación de privilegios	Alta	libufdt
CVE-2022-42531	A-231500967 *	Elevación de privilegios	Alta	TF-A
CVE-2022-20562	A-231630423 *	Divulgación de información	Alta	Audio processor
CVE-2022-20574	A-237582191 *	Divulgación de información	Alta	LDFW
CVE-2022-20575	A-237585040 *	Divulgación de información	Alta	LDFW
CVE-2022-20602	A-211081867 *	Divulgación de información	Alta	Modem
CVE-2022-20604	A-230463606 *	Divulgación de información	Alta	Exynos Firmware
CVE-2022-20608	A-239239246 *	Divulgación de información	Alta	Cellular firmware
CVE-2022-42529	A-235292841 *	Divulgación de información	Alta	Kernel
CVE-2022-42530	A-242331893 *	Divulgación de información	Alta	Pixel firmware
CVE-2022-42532	A-242332610 *	Divulgación de información	Alta	Pixel firmware
CVE-2022-20563	A-242067561 *	Elevación de privilegios	Moderada	Bootloader

CVE-2022-20569	A-229258234 *	Elevación de privilegios	Moderada	Pixel Thermal Control Driver
CVE-2022-20576	A-239701761 *	Elevación de privilegios	Moderada	Telephony
CVE-2022-20577	A-241762281 *	Elevación de privilegios	Moderada	sitril
CVE-2022-20578	A-243509749 *	Elevación de privilegios	Moderada	rild_exynos
CVE-2022-20579	A-243510139 *	Elevación de privilegios	Moderada	rild_exynos
CVE-2022-20580	A-243629453 *	Elevación de privilegios	Moderada	libufdt
CVE-2022-20581	A-245916120 *	Elevación de privilegios	Moderada	Pixel camera driver
CVE-2022-20594	A-239567689 *	Elevación de privilegios	Moderada	Wireless Charger
CVE-2022-20596	A-239700400 *	Elevación de privilegios	Moderada	Wireless Charger
CVE-2022-20600	A-239847859 *	Elevación de privilegios	Moderada	LWIS
CVE-2022-42501	A-241231403 *	Elevación de privilegios	Moderada	rild_exynos
CVE-2022-42502	A-241231970 *	Elevación de privilegios	Moderada	rild_exynos
CVE-2022-42503	A-241231983 *	Elevación de privilegios	Moderada	rild_exynos
CVE-2022-42504	A-241232209 *	Elevación de privilegios	Moderada	rild_exynos
CVE-2022-42505	A-241232492 *	Elevación de privilegios	Moderada	rild_exynos
CVE-2022-42506	A-241388399 *	Elevación de privilegios	Moderada	rild_exynos
CVE-2022-42507	A-241388774 *	Elevación de privilegios	Moderada	rild_exynos
CVE-2022-42508	A-241388966 *	Elevación de privilegios	Moderada	rild_exynos
CVE-2022-42509	A-241544307 *	Elevación de privilegios	Moderada	rild_exynos
CVE-2022-42510	A-241762656 *	Elevación de privilegios	Moderada	rild_exynos
CVE-2022-42511	A-241762712 *	Elevación de privilegios	Moderada	rild_exynos
CVE-2022-42513	A-241763204 *	Elevación de privilegios	Moderada	rild_exynos
CVE-2022-42518	A-242536278 *	Elevación de privilegios	Moderada	rild_exynos

CVE-2022-42519	A-242540694*	Elevación de privilegios	Moderada	rild_exynos
CVE-2022-42520	A-242994270*	Elevación de privilegios	Moderada	rild_exynos
CVE-2022-42521	A-243130019*	Elevación de privilegios	Moderada	rild_exynos
CVE-2022-42523	A-243376893*	Elevación de privilegios	Moderada	rild_exynos
CVE-2022-42525	A-243509750*	Elevación de privilegios	Moderada	rild_exynos
CVE-2022-42526	A-243509880*	Elevación de privilegios	Moderada	rild_exynos
CVE-2022-20560	A-212623833*	Divulgación de información	Moderada	Kernel
CVE-2022-20570	A-230660904*	Divulgación de información	Moderada	Modem
CVE-2022-20593	A-239415809*	Divulgación de información	Moderada	gralloc
CVE-2022-20595	A-239700137*	Divulgación de información	Moderada	Wireless Charger
CVE-2022-20601	A-204541506*	Divulgación de información	Moderada	Modem
CVE-2022-20605	A-231722405*	Divulgación de información	Moderada	Modem
CVE-2022-20606	A-233230674*	Divulgación de información	Moderada	Modem
CVE-2022-20609	A-239240808*	Divulgación de información	Moderada	Cellular firmware
CVE-2022-42512	A-241763050*	Divulgación de información	Moderada	rild_exynos
CVE-2022-42514	A-241763298*	Divulgación de información	Moderada	rild_exynos
CVE-2022-42515	A-241763503*	Divulgación de información	Moderada	rild_exynos

CVE-2022-42516	A-241763577 *	Divulgación de información	Moderada	rild_exynos
CVE-2022-42517	A-241763682 *	Divulgación de información	Moderada	rild_exynos
CVE-2022-42522	A-243130038 *	Divulgación de información	Moderada	rild_exynos
CVE-2022-42524	A-243401445 *	Divulgación de información	Moderada	Modem
CVE-2022-42527	A-244448906 *	Denegación de servicio	Moderada	Modem

Componentes Qualcomm

CVE	Referencias	Severidad	Subcomponente
CVE-2022-25677	A-235114749 QC-CR#3122626 QC-CR#3103567	Moderada	Bootloader

Componentes Qualcomm de código cerrado

CVE	Referencias	Severidad	Subcomponente
CVE-2021-30348	A-202032128 *	Moderada	Componente de código cerrado
CVE-2022-25675	A-208302286 *	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: diciembre 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

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA