

Android-en segurtasun eguneraketa – 2022ko otsaila

BCSC-EGUNERAKETAK-ANDROID-2022-OTSAILA

TLP:WHITE

www.basquecybersecurity.eus



2022ko otsaila

AURKIBIDEA

BCSC-ri buruz	3
1. Laburpen exekutiboa	4
2. Kaltetutako baliabideak	5
3. Azterketa teknikoa	6
4. Arintzea / Konponbidea	9
5. Erreferentzia osagarriak	10

Erantzukizunetik salbuesteari buruzko klausula

Honako dokumentu hau eskaintzen da erakundeen eta interesa duten herritarren segurtasunerako BCSCk beharrezkotzat jotzen dituen alertak ezagutzera emateko. Inongo kasutan BCSC ezin da kontsideratu hemen zabaldutako informazioaren erabilpenak zuzenean nahiz zeharka, ustekabeen nahiz modu berezian, eragin litzakeen balizko kalteen arduradun. Gauza bera esan beharra dago BCSCren webean edo hortik esteken bitartez joan litekeen kanpoko web orrialdeetan, sare sozialetan, software produktuetan edo alertan nahiz BCSCren webean agertutako beste edozein informaziotan aipa litezkeen teknologiei dagokienez. Edozein kasutan, alertaren edukiak eta mezu elektronikoen bidez eman litezkeen erantzunak hemen jasotako terminoetan emandako iritzi eta gomendioak dira eta jakinarazitako informaziotik ezin da ondorioztatu ondorio juridiko loteslerik.

Salmenta debekatzeari buruzko klausula

Guztiz debekatuta dago dokumentu hau saltzea edo beragatik edozein onura ekonomiko eskuratzea, baina posible da bera kopiazea, banatzea, hedatzea edo ezagutzera ematea.

BCSC-RI BURUZ

Zibersegurtasunaren Euskal Zentroa (Basque Cybersecurity Centre, BCSC) Eusko Jaurlaritzak zibersegurtasunaren heldutasun-maila handitzeko izendatutako erakundea da.

Zeharkako ekimena da, Eusko Jaurlaritzako Ekonomiaren Garapen, Jasangarritasun eta Ingurumen Sailaren mendekoa den Enpresen Garapenerako Euskal Agentziaren (SPRI) barruan dagoena. Era berean, Eusko Jaurlaritzako beste hiru sail ere sartzen dira ekimenean –Segurtasuna, Gobernantza Publikoa eta Autogobernua eta Hezkuntza Saila–, eta Zientzia, Teknologia eta Berrikuntzaren Euskal Sareko lau eragile: Tecnalia, Vicomtech, Ikerlan eta BCAM.



BCSC erreferentzia-erakundea da Euskadiko herritarren, enpresen eta erakunde publikoen zibersegurtasuna eta konfiantza digitala garatzeko, bereziki eskualdeko ekonomiaren sektore estrategikoentzat.

BCSCren egitekoa da, beraz, euskal gizartean zibersegurtasuna sustatzea eta garatzea, Euskadiko enpresa-jarduera dinamizatzea eta erreferentzia izango den sektore profesional bat sortzea ahalbidetzea. Testuinguru horretan, eragile osagarrien arteko lankidetzak-proiektuak gauzatzea bultzatzen da, berrikuntza teknologikoaren, ikerketaren eta fabrikazio aurreratuko industriarako eta beste sektore batzuetarako transferentzia teknologikoaren eremuetan.

Era berean, hainbat zerbitzu eskaintzen ditu Gorabeheri erantzuteko lantalde gisa (aurrerantzean CERT: “Computer Emergency Response Team” ingelesezko siglak), eta Euskal Autonomia Erkidegoaren esparruan lan egiten du mehatxu berriak detektatzeko eta garaiz ohartarazteko gaitasuna handitzen, informazioaren segurtasun-gorabeheren erantzuna eta analisia egiten, eta euskal gizartearen beharrei erantzuteko prebentzio-neurriak diseinatzeko. Helburu horiek lortzeko, zibersegurtasun-gorabeherak kudeatzera bideratutako hainbat ekimenen parte da:



1. LABURPEN EXEKUTIBOA

Googlek 2022ko otsailari dagozkion Android-en segurtasun eguneraketak argitaratu ditu. Horiekin sistema eragilearen 10, 11 eta 12 bertsioen 38 ahultasun konpontzen dira, bai eta Google gailuei eragiten dieten beste 4 ahultasun ere, Pixel 3tik Pixel 6ra bitarteko modeloetan.

Androiden zuzendutako 38 ahultasunetatik 2ri larritasun kritikoa esleitu zaie eta gainerakoei larritasun altua. Google Pixel gailuetan zuzendutako ahultasunei dagokienez, bik daukate larritasun altua eta beste bik ertaina.

Arriskuak saihesteko eguneraketak azkar ezartzea gomendatzen da.

2. KALTETUTAKO BALIABIDEAK

2022ko otsaileko Android-en segurtasun eguneraketek honako produktu hauei eragiten dieten ahultasunekin daukate zerikusia:

- Framework
- Media Framework
- Sistema
- Google Play-ren sistemaren eguneraketak
- Amlogic osagaiak
- Mediatec osagaiak
- Unisoc osagaiak
- Qualcomm osagaiak

3. AZTERKETA TEKNIKOA

Ondoren doa kaltetutako sistema bakoitzari dagokion eta zuzendu diren ahultasun guztien zerrenda:

Framework:

CVE	Mota	Larritasuna	Bertsioak
CVE-2021-39619	Pribilegioen igoera	Altua	11, 12
CVE-2021-39662	Pribilegioen igoera	Altua	11, 12
CVE-2021-39663	Pribilegioen igoera	Altua	10
CVE-2021-39676	Pribilegioen igoera	Altua	11
CVE-2021-39664	Informazioa zabaltzea	Altua	12

Media Framework

CVE	Mota	Larritasuna	Bertsioak
CVE-2020-13112	Pribilegioen igoera	Altua	10, 11
CVE-2020-13113	Pribilegioen igoera	Altua	10, 11
CVE-2021-39665	Informazioa zabaltzea	Altua	12
CVE-2021-39666	Informazioa zabaltzea	Altua	11, 12

Sistema

CVE	Mota	Larritasuna	Bertsioak
CVE-2021-39675	Pribilegioen igoera	Kritikoa	12
CVE-2021-39668	Pribilegioen igoera	Altua	11, 12
CVE-2021-39669	Pribilegioen igoera	Altua	11, 12
CVE-2021-39671	Pribilegioen igoera	Altua	12
CVE-2021-39674	Pribilegioen igoera	Altua	10, 11, 12
CVE-2021-0706	DoS	Altua	10, 11

Google Play-ren sistemaren eguneraketak

Osagaia	CVE
Media Provider	CVE-2021-39662, CVE-2021-39663

Sistema

CVE	Mota	Larritasuna	Bertsioak
CVE-2021-39631	Informazioa zabaltzea	Altua	10, 11, 12

Amlogic osagaiak

CVE	Larritasuna	Osagaia
CVE-2021-39672	Altua	Fastboot

MediaTek osagaiak

CVE	Larritasuna	Osagaia
CVE-2022-20024	Altua	Sistemaren zerbitzua
CVE-2022-20025	Altua	Bluetooth
CVE-2022-20026	Altua	Bluetooth
CVE-2022-20027	Altua	Bluetooth
CVE-2022-20028	Altua	Bluetooth

Unisoc osagaiak

CVE	Larritasuna	Osagaia
CVE-2021-39616	Altua	sprd-vowifi
CVE-2021-39635	Altua	ims_ex
CVE-2021-39658	Altua	IsmsEx

Qualcomm osagaiak

CVE	Larritasuna	Osagaia
CVE-2021-35068	Altua	Bluetooth
CVE-2021-35069	Altua	WLAN
CVE-2021-35074	Altua	Kernel
CVE-2021-35075	Altua	Kernel
CVE-2021-35077	Altua	Kernel

Kode itxiko Qualcomm osagaiak

CVE	Larritasuna	Osagaia
CVE-2021-30317	Kritikoa	Kode itxiko osagaia
CVE-2021-30309	Altua	Kode itxiko osagaia
CVE-2021-30318	Altua	Kode itxiko osagaia
CVE-2021-30322	Altua	Kode itxiko osagaia
CVE-2021-30323	Altua	Kode itxiko osagaia
CVE-2021-30326	Altua	Kode itxiko osagaia

Google Pixel gailuak

CVE	Mota	Larritasuna	Osagaia
CVE-2021-39687	Informazioa zabaltzea	Altua	Kamera
CVE-2021-39688	Informazioa zabaltzea	Altua	Google bateria

Qualcomm osagaiak

CVE	Larritasuna	Osagaia
CVE-2021-30324	Ertaina	Kernel
CVE-2021-30325	Ertaina	Kernel

4. ARINTZEA / KONPONBIDEA

Ahultasun guztiak arintzeko eta partxatzeko Googlek dagozkien segurtasun eguneraketak argitaratzen ditu [arintze oharrekin](#) batera, [Androiden Segurtasun Buletinetan](#) eskuragarri daudenak.

5. ERREFERENTZIA OSAGARRIAK

- [Androiden segurtasun buletina: 2021eko otsaila | Android Open Source Project](#)
- [Segurtasun baliabideak eta eguneraketak | Android Open Source Project](#)
- [Software eguneraketen epeak Google Pixel telefonoetan - Pixel Phone-ren laguntza](#)
- [Google-Android komunitate ofiziala](#)



Gertakarien jakinarazpena

Zibersegurtasun gertakariaren bat aurkitu baduzu jakinaraz diezaguzu, horrela beharrezkoak diren neurriak hartuko ditugu zabal ez dadin.

900 104 891

arazoak@bcsc.eus

Zibersegurtasun katalogoa

Zure zibersegurtasunarekin edo zure enpresarenarekin laguntza behar duzu?

