Basque CyberSecurity Centre

Zero-day Apple iOS e iPadOS kalteberatasuna (CVE-2022-42827)

BCSC-ABISUAK

TLP: CLEAR

www.zibersegurtasun.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

EDUKIAREN TAULA

Erantzukizunetik salbuesteko klausula

Dokumentu hau ematen da BCSCk erakundeen eta herritar interesdunen segurtasunaren alde beharrezkotzat jotzen dituen alertak zabaltzeko. BCSC ezin da inola ere jo zuzenean edo zeharka, ustekabean edo ohiz kanpo jakinarazitako informazioa erabiltzeak eragin ditzakeen kalteen erantzuletzat, ez eta BCSCren webgunetik nahiz kanpoko informaziotik (kanpoko web-orrietarako, sare sozialetarako, software-produktuetarako edo BCSCren alertaren edo webgunearen bidez ager daitekeen beste edozein informaziotarako esteken bidez) aipatzen diren teknologien erantzuletzat ere. Nolanahi ere, alertaren edukiak eta mezu elektronikoen bidez eman daitezkeen erantzunak hemen jasotako baldintzen araberako iritziak eta gomendioak dira, eta ezingo da ondorio juridiko loteslerik sortu jakinarazitako informaziotik.

Saltzeko debekuaren klausula

Guztiz debekatuta dago saltzea edo edozein onura ekonomiko lortzea, dokumentu hau kopiatzeko, banatzeko, hedatzeko nahiz zabaltzeko aukera alde batera utzi gabe.

BCSCri 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 erreferentea izango den sektore profesional bat sortzea ahalbidetzea. Testuinguru horretan, eragile osagarrien arteko lankidetza-proiektuak gauzatzea bultzatzen da, berrikuntza teknologikoaren, ikerketaren eta fabrikazio aurreratuko industriarako eta beste sektore batzuetarako transferentzia teknologikoaren eremuetan.

Era berean, hainbat zerbitzu eskaintzen ditu Gorabeherei 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 diseinatzen. Helburu horiek lortzeko, zibersegurtasun-gorabeherak kudeatzera bideratutako hainbat ekimenen parte da:

FIRST Improving Security Together
TF-CSIRT Trusted Introducer
CSIRT.es

1. Segurtasun-abisua

Apple-k zero-day kalteberatasun bat informatu du CVE-2022-42827 identifikatzailearekin. Kalteberatasunak bere IPhone eta IPad gailuen Kernelari eragiten dio, eta oraindik ez dago informazio zehatzik argitaratuta. Konpainiak berak dio hirugarrenen txosten batzuen berri duela, eta txosten horietan ziurtatzen dela arazo hori **aktiboki ustiatu ahal izan dela**.

2. Eragindako baliabideak

- iPhone 8 eta ondorengo bertsioak.
- iPad Pro modelo guztiak.
- 3. belaunaldiko iPad Air eta ondorengo bertsioak.
- 5. belaunaldiko iPad eta ondorengo bertsioak.
- 5. belaunaldiko iPad mini eta ondorengo bertsioak.

3. Analisi teknikoa

CVE-2022-42827 gisa identifikatutako kalteberatasuna bat dator uneko memoriaren bufferraren mugetatik kanpo datuak idazten dituen softwarearen mugetatik kanpoko idazketaren arazoarekin; beraz, aplikazio batek kode arbitrarioa exekuta dezake Kernel pribilegioekin.

4. Arintzea / Konponbidea

Kalteberatasun hori arintzeko, BCSCk gomendatzen du sistema eta aplikazioak erabilgarri dagoen azken bertsiora eguneratuta edukitzea beti, dagozkion eguneraketak argitaratu bezain laster.

Horregatik, hutsegitearen kritikotasuna dela-eta, enpresak emandako eguneratzea aplikatzea gomendatzen da; hau da, eragindako gailuen eguneraketa instalatzea iOS 16.1 bertsiorako (bertsio horretan sartzen dira iOS gailuak kodea exekutatzeko erasoen esposiziopean jartzen dituzten gutxienez lau arazo gehigarritarako zuzenketak ere: CVE-2022-32922, CVE-2022-42823, CVE-2022-42808, CVE-2022-42813), eta iPadOS 16rako.

5. Erreferentzia gehigarriak https://support.apple.com/es-es/HT213341

- CVE-2022-42827
- CVE-2022-32922
- CVE-2022-42823
- CVE-2022-42808
- CVE-2022-42813
- Apple Security Updates
- https://www.securityweek.com/apple-fixes-exploited-zero-day-ios-161-patch
- https://www.bleepingcomputer.com/news/apple/apple-fixes-new-zero-day-used-in-attacks-against-iphones-ipads/

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA