Basque CyberSecurity Centre

Zero-day ahultasunak Applen

TLP: CLEAR

www.zibersegurtasun.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

AURKIBIDEA

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, ustekabean 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

BCSC-ri buruz

Zibersegurtasun Euskal Zentroa (Basque Cybersecurity Centre, BCSC) da Eusko Jaurlaritzak izendatutako entitatea Euskadin zibersegurtasunaren gaian heldutasun maila igotzeko.

Zeharkako ekimena da, Enpresa Garapenerako Euskal Agentziaren (SPRI) barnean kokatua, Eusko Jaurlaritzako Ekonomiaren Garapen, Jasangarritasun eta Ingurumen Sailaren menpe dagoen sozietatea. Era berean, Eusko Jaurlaritzako beste hiru Sail ere bere parte dira: Segurtasuna, Gobernantza Publiko eta Autogobernua, eta Hezkuntza; bai eta Zientzia, Teknologia eta Berrikuntzako Euskal Sistemako lau eragile ere: Tecnalia, Vicomtech, Ikerlan eta BCAM.

BCSC erreferentziazko entitatea da zibersegurtasuna eta konfiantza digitala garatzeko Euskadiko herritar, enpresa eta instituzio publikoen artean, eta batez ere, eskualdeko ekonomiaren sektore estrategikoen kasuan.

Beraz, BCSCren eginkizuna da euskal gizartean zibersegurtasuna sustatzea eta garatzea, Euskadiko enpresa jarduera dinamizatzea, eta erreferentzia izango den sektore profesional bat sor dadin eragitea. Testuinguru horretan osagarriak diren eragileen arteko lankidetza proiektuak exekutatzea sustatzen du, berrikuntza teknologikoaren, ikerkuntzaren, eta fabrikazio aurreratuko industriarako eta beste sektore batzuetarako transferentzia teknologikoaren alorretan.

Era berean, hainbat zerbitzu eskaintzen ditu Gertakarien Aurreko Ekipo modura duen rolagatik (aurrerantzean CERT, ingeleseko izenaren siglak direla-eta “Computer Emergency Response Team”). Euskal Autonomia Erkidegoko esparruan mehatxu berriak antzemateko eta horiei buruzko alerta goiztiarrak emateko gaitasuna areagotzen dihardu lanean, informazioaren segurtasun gertakarien erantzunean eta analisian, eta euskal gizartearen beharrak artatzeko beharrezkoak diren prebentzio neurrien diseinuan. Helburu horiek lortzeko xedearekin, zibersegurtasun gertakariak kudeatzera zuzendutako hainbat ekimenetan hartzen du parte:

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

1. Laburpen exekutiboa

Applek hainbat segurtasun abisu argitaratu ditu. Horietan, zero-day motako hiru ahultasun lantzen dira, WebKit osagaian dauden akatsen ondorio direnak, eta iOS, iPadOS, macOS Ventura, macOS Monterey, macOS Big Sur, watchOS eta tvOS sistemei eragiten dietenak. CVE-2023-32409, CVE-2023-28204 eta CVE-2023-32373 zenbakiekin identifikatutako ahultasunek oraingoz ez dute puntuaziorik CVSSv3 eskalaren arabera, baina fabrikatzaileak zero-day motakotzat kalifikatu ditu, eta, beraz, zorroztasun kritikoa ematen zaie. Izan ere, uste da akatsak modu aktiboan ustiatzen ari direla sarean, baina ez da detektatu ahultasun horiek aprobetxatzen dituen ustiapenik argitaratu denik.

Zero-day akats berri horiek helmugako sistemaren konpromiso osoa izan daitezke, eta ustiapen arrakastatsu batek urruneko erasotzaile bati aukera eman liezaioke datuen ustelkeria eragiteko, gailuaren edukia irakurtzeko eta kode arbitrarioa exekutatzeko gaitasuna eskuratzeko. Akats nabarmenak ustiatzeak izan ditzakeen ondorio larrien arabera, Applek emandako arintze-jarraibideak betetzea da irtenbidea.

Fabrikatzaileak dagoeneko argitaratu ditu dagozkion eguneratzeak, eta, horrela, akats kritiko nabarmenak zuzendu ditu. Hori dela eta, ahultasun horiek eta beste batzuk prebenitzeko, sistema eta aplikazioak eskuragarri dagoen azken bertsioan eguneratuta izatea gomendatzen da, dagozkien adabakiak argitaratu bezain laster.

2. Azterketa teknikoa

Lehen ahultasun nabarmena CVE-2023-32409n identifikatu da, eta sistema kalteberaren WebKit osagaiari eragiten dio, aplikazioan web-edukia hainbat estilorekin integratzeko ardura baitu. Zehazkiago, aipatutako errore horrek ahalbidetzen du urruneko erasotzaile batek helmugako sisteman kode arbitrarioa exekutatu ahal izatea. Ahultasuna WebKit plataforma anitzeko nabigazio-motorraren boundary akats baten ondorioz dago. Mehatxu-eragile batek erabiltzailea engainatzeko aukera du, webgune maltzur bat bisitatzeko, gailuaren memoria galarazteko eta sistemaren web-edukiaren sandboxa saihesteko.

CVE-2023-28204n erregistratutako akatsari dagokionez, *WebKit* osagaiari ere eragiten dio. Akats horri esker, erasotzaile bat sentibera izan daitekeen informaziora sar daiteke. Ahultasuna osagai nabarmeneko *boundary errore* batek eragiten du. Erasotzaile batek erabiltzailea engaina dezake web gune maltzur bat bisitatzeko, *out-of-bounds read error* bat eragiteko eta helburu-sistemaren memorian gordetako edukia kontsultatzeko.

CVE-2023-32373-ren bidez identifikatutako akatsari dagokionez, mehatxu-eragile batek sistema objektiboa erabat arriskuan jar dezake. Akatsa gertatu da *WebKit-en* gertatzen den *use-after-free* errore baten ondorioz. Urruneko erasotzaile batek biktima engaina dezake, bereziki diseinatutako web orri batera joan dadin, akats nabarmena eragin dezan eta sisteman kode arbitrarioa erabil dezan.

Ahultasun horiek modu aktiboan ustiatzen ari diren zantzuak daudela esan behar da, baina, lehenago esan den bezala, enpresak ez ditu gertaera maltzurrei buruzko xehetasunak partekatu. Izan ere, Appleren helburua da teknika berriak edo kontzeptu probak (PoC) garatzea, erabiltzaileek gailu ahuletan Segurtasun eguneratzeak aplikatzen dituzten bitartean akats hori ustiatu ahal izateko.

Azkenik, ahultasun horiek bertsio hauei eragiten diete:

- iPhone 6s modelo guztiak.
- iPhone 7-ko modelo guztiak.
- 1. belaunaldiko iPhone SE.
- iPhone 8 eta ondorengoak.
- iPad Air 2 modelo guztiak.
- 4. belaunaldiko iPad minia.
- iPad Pro modelo guztiak.
- 3. belaunaldiko eta ondorengo iPad Air.
- 5. belaunaldiko eta hurrengoetako iPad.

- iPad minia, 5. belaunaldikoa eta hurrengoetakoa.
- 7. belaunaldiko iPod Touch.
- Mac makOS Big Sur, Monterey eta Venturarekin.
- Apple Watch 4. seriea eta ondorengoak.
- Apple TV 4K-ko modelo guztiak.
- Apple TV HD.

3. Arintzea / Mitigazioa

Ohikoa denez, ahultasun horiek eta beste batzuk prebenitzeko, sistemak eta aplikazioak eskuragarri dagoen azken bertsioan eguneratuta izatea gomendatzen da, dagozkion eguneratzeak argitaratu bezain laster.

Oso garrantzitsua da neurriak azkar hartzea akats nabarmenak konpontzeko. Horregatik, ahultasunen larritasuna dela eta, konpainiak emandako eguneratzeak aplikatzea gomendatzen da, iOS eta iPadOS 16.5 edo 15.7.6 bertsioari eta macOS Ventura 13.4 bertsioari eguneratuz, macOS Monterey 12.6.6 bertsioari, macOS Big Sur 11.7.7 bertsioari, Safari 16.5 bertsioari, watchOS 9.5 bertsioari eta tvOS 16.5 bertsioari.

Aipatutako eguneratzeak esteka honen bidez aurki daitezke:

- https://developer.apple.com/news/releases/

Instalazioa errazteko, fabrikatzaileak emandako jarraibideei jarraitzea gomendatzen da. Hona hemen jarraibideok:

- https://support.apple.com/es-es/HT204204
- https://support.apple.com/es-es/HT201541
- https://support.apple.com/es-es/HT204641
- https://support.apple.com/es-es/HT202716

Zero-day motako hiru ahultasun direnez, Appleren taldeak biziki gomendatzen die erabiltzaileei produktu horiek ahalik eta azkarren eguneratzeko.

4. Erreferentzia osagarriak

- Segurtasun oharrak
- CVE-2023-32409.
- CVE-2023-28204.
- CVE-2023-32373.
- WebKit.
- Boundary error.
- App Sandbox.
- CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer.
- CWE-125: Out-of-bounds Read.
- CWE-416: Use After Free.
- Apple: News and Updates.
- iPhone edo iPad eguneratu.
- MacOS eguneratu Mac-en.
- Apple Watch eguneratu.
- Apple TV eguneratu.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA