# Zero-day kalteberatasunak Appleren iOS eta iPadOS-en

CYBERZAINTZA-ABISUAK

**TLP: CLEAR**

www.zibersegurtasun.eus

EUSKO JAURLARITZA
GOBIERNO VASCO

## EDUKI-TAULA



## Erantzukizunetik salbuesteko klausula



## Salmenta debekatzeko klausula

## 1. Laburpen exekutiboa

**Applek** segurtasun-abisuak argitaratu ditu zero-day motako **2 kalteberatasuni** buruz. **iOS eta iPadOS-en kernelari** eta **RTKit** osagaiari eragiten diete kalteberatasun horiek. Honako hauek dira kalteberatasun horien identifikatzaileak: CVE-2024-23225 eta CVE-2024-23296. Eta memoriaren korrupzioa eragiten dute.

Arazo horiek **aktiboki ustiatu** direla adierazten duen txostenen berri duela baieztatu du Applek.

Kalteberatasunei, momentuz, ez zaie CVSSv3 eskalako puntuaziorik eman, baina fabrikatzaileak zero-day erakotzat kalifikatu ditu; hortaz, **larritasun kritikoa** ezarri zaie.

Fabrikatzaileak dagoeneko argitaratu ditu dagozkion eguneratzeak eta arintze-neurriak, eta, horrela, akats nabarmenak zuzendu ditu. Beraz, kalteberatasun horiek eta beste batzuk prebenitzeko, sistema eta aplikazioak eskuragarri dagoen azken bertsioaren arabera eguneratuta izatea gomendatzen da, dagozkien adabakiak argitaratu bezain laster.

## 2. Kaltetutako baliabideak

- iOS 17.4 eta iPadOS 17.4 duten produktu hauek:

  iPhone XS eta hurrengoak, 12.9 hazbeteko 2. belaunaldiko iPad Pro eta hurrengoak, 10.5 hazbeteko iPad Pro, 11 hazbeteko 1. belaunaldiko iPad Pro eta hurrengoak, 3. belaunaldiko iPad Air eta hurrengoak, 6. belaunaldiko iPad eta hurrengoak, eta 5. belaunaldiko iPad mini eta hurrengoak.

- iOS 16.7.6 eta iPadOS 16.7.6 duten produktu hauek:

  iPhone 8, iPhone 8 Plus, iPhone X, 5. belaunaldiko iPad, 9.7 hazbeteko iPad Pro eta 12.9 hazbeteko 1. belaunaldiko iPad Pro.

## 3. Azterketa teknikoa

Abisu honetan landutako kalteberatasunen **(baliteke ustiatu izana)** xehetasunak dira honako hauek:

CVE-2024-23225: memoriaren korrupzioan oinarritutako kalteberatasuna. Kernela irakurtzeko eta bertan idazteko gaitasun arbitrarioa duen erasotzaile batek kerneleko memoriaren babesak saihestu ditzake.

CVE-2024-23296: memoriaren korrupzioan oinarritutako kalteberatasuna. Kernela irakurtzeko eta bertan idazteko gaitasun arbitrarioa duen erasotzaile batek kerneleko memoriaren babesak saihestu ditzake.

## 4. Arintzea / Konponbidea

Ohikoa den bezala, kalteberatasun horiek eta beste batzuk prebenitzeko, sistemak eta aplikazioak beti eskuragarri dagoen azken bertsiora eguneratuta izatea gomendatzen da, dagozkien eguneratzeak argitaratu bezain laster.

Garrantzitsua da nabarmendutako akatsak konpontzeko neurriak azkar hartzea. Hori dela eta, kalteberatasunen larritasuna aintzat hartuta, enpresak emandako eguneratzeak aplikatzea eta, hala, iOS eta iPadOS sistema eragileak eguneratzea gomendatzen da.

Aipatutako eguneratzeak esteka honen bidez lor litezke:

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

Instalazioa errazteko, fabrikatzaileak eskainitako ondoko jarraibideak segitzea gomendatzen da:

- https://support.apple.com/es-es/HT204204

**Zero-day** erako **kalteberatasunak** direnez, produktu horiei dagozkien eguneratzeak lehenbailehen egitea gomendatzen die Appleko lantaldeak erabiltzaileei.

## 5. Erreferentzia gehigarriak

- Segurtasun-abisuak.
- CVE-2024-23225.
- CVE-2024-23296.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY