



# Mozilla Firefox, Firefoz ESR eta Thunderbirdeko kalteberatasunak

CYBERZAINITZA-ABISUAK

**TLP: CLEAR**

[www.zibersegurtasun.eus](http://www.zibersegurtasun.eus)



## EDUKI-TAULA

---

1. Laburpen exekutiboa .....	3
2. Kaltetutako baliabideak .....	4
3. Azterketa teknikoa .....	5
4. Arintzea / Konponbidea .....	7
5. Erreferentzia gehigarriakSegurtasun-abisuak. ....	8

## Erantzukizunetik salbuesteko klausula

---

Dokumentu hau Zibersegurtasunaren Euskal Agentziak erakundeen eta herritar interesatuen segurtasunaren alde beharrezkotzat jotzen dituen alertak gizarteratzeko helburuz sortu da. Zibersegurtasunaren Euskal Agentzia ezin da jo, inola ere, Zibersegurtasunerako Euskal Agentziaren webgunean emandako informazioaren edo erreferentzia egiten zaien teknologien erabilerak eragin ditzaketen kalteen erantzuletzat, ezta kanpoko web-orrialdeetarako esteka bidez sartutako bestelako informazioaren, software produktuen edo Zibersegurtasunaren Euskal Agentziaren webgunean edo alertan ager daitezkeen beste edozein informazioaren erantzuletzat ere. Edonola ere, alertaren edukiak eta mezu elektronikoen bidez eman litezkeen erantzunak iritzi eta gomendioak dira, hemen bildutako terminoekin bat etorrira, eta emandako informazioaren ondorioz ezingo da eragin juridiko loteslerik sortu.

## Salmenta debekatzeko klausula

---

Gutziz debekatuta dago saltzea edo edozein etekin ekonomiko lortzea, baina horrek ez du eragotziko dokumentu hau kopiatzeko, banatzeko, zabaltzeko edo gizarteratzeko aukera.

## 1. Laburpen exekutiboa

---

Mozillak [segurtasun-abisuak](#) igorri ditu. **Firefox** nabigatzailea, **Firefox ERS** eta **Mozilla Thunderbird** multiplataformaren posta elektronikoa darabilen bezeroari eragiten dieten hainbat kalteberatasun lantzen dira bertan.

Kalteberatasun horien barruan, **1 kalteberatasun kritikokoa** da, [CVE-2024-2615](#) identifikatzailea duena, eta beste zazpi **kalteberatasun handikoak**, honako identifikatzaile hauekin: [CVE-2024-2614](#), [CVE-2024-2608](#), [CVE-2024-2607](#), [CVE-2024-2606](#), [CVE-2024-2605](#), [CVE-2024-2616](#) eta [CVE-2024-0743](#) .

Kalteberatasun horiek ustiatuz gero, [Heapean oinarritutako buferrak gainezka egin dezake](#) eta [kodea modu arbitrarioan exekutatu daiteke](#), besteak beste.

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

---

- Mozilla Firefoxen 124 bertsioaren aurrekoak.
- Firefox ESR 115.9 bertsioaren aurrekoak.
- Firefox Thunderbird 115.9.0 bertsioaren aurrekoak.

### 3. Azterketa teknikoak

---

Abisu honetan landutako kalteberatasunen xehetasunak hauek dira:

**Larritasun kritikoa** duen [CVE-2024-2615](#) kalteberatasunak Firefox 123ri eragiten dio. Firefox 123 bertsioaren memorian dauden segurtasun-akatsak eragindakoa da. Akats horietako batzuek memoriaren ustelkeriaren zantzuak erakusten dituzte eta ustiatuz gero, kodea modu arbitrarioan exekutatu daiteke. Kalteberatasunak Firefoxen 124 bertsioaren aurrekoei eragiten dio.

[CVE-2024-2614](#) kalteberatasunak Firefoxen 124 bertsioaren aurreko bertsioei, Firefox ESRren 115.9 bertsioaren aurreko bertsioei eta Thunderbirden 115.9 bertsioaren aurreko bertsioei eragiten die. Memorian presente dauden segurtasun-akatsak eragin dute errorea eta ustelkeriaren ebidentziak daudela erakutsi dute. **Baliteke hori ustiatu izana** eta kode arbitrarioa exekutatzeko aukera eman izana.

[CVE-2024-2605](#) kalteberatasunak Firefoxen 124 bertsioaren aurreko bertsioei, Firefox ESRren 115.9 bertsioaren aurreko bertsioei eta Thunderbirden 115.9 bertsioaren aurreko bertsioei eragiten die. Windows Error Reportes sandboxeko ihes-bektore gisa erabiltzeko aukera hauteman da, sisteman kode arbitrarioa exekutatuz. **Arazo horrek Windowseko sistema operatiboari soilik eragiten die.**

Jarraian, [CVE-2024-2606](#) kalteberatasunak Firefoxen 124 bertsioaren aurreko bertsioei eragiten die. Balio gabeko datuak pasatzeagatik, baliteke warm balio baliogabeak sortu izana puntako balioak bihurtzen diren osoko arbitrario gisa.

Argitaratutako [CVE-2024-2607](#) kalteberatasunak Firefoxen 124 bertsioaren aurreko bertsioei, Firefox ESRren 115.9 bertsioaren aurreko bertsioei eta Thunderbirden 115.9 bertsioaren aurreko bertsioei eragiten die. Itzultzeko erregistroen gainean idatzi dela hauteman da. Horren ondorioz, baliteke erasotzaile batek kode arbitrarioa exekutatzeko aukera izatea. **Arazoak Armv7-A arkitekturari soilik eragiten dio.**

[CVE-2024-2608](#) kalteberatasunak Firefoxen 124 bertsioaren aurreko bertsioei, Firefox ESRren 115.9 bertsioaren aurreko bertsioei eta Thunderbirden 115.9 bertsioaren aurreko bertsioei eragiten die. Hauteman da osokoek gainezka egin dutela `AppendEncodedAttributeValue()`, `ExtraSpaceNeededForAttrEncoding()` eta `AppendEncodedCharacters()` funtzioetan. Horren ondorioz, irteera-bufferra gainesleitu daiteke eta horrek mugez kanpo idaztea eragin dezake.

[CVE-2024-2616](#) kalteberatasunak Firefox ESRren 115.9 bertsioaren aurreko bertsioei eta Thunderbirden 115.9 bertsioaren aurreko bertsioei eragiten die. Kalteberatasunaren jatorria da Javan eta C/C++n erabiltzen diren ICU liburutegien multzoaren aurkako ustiapena indartzeko saiakera. Jokabidea

aldatu da memoria faltagatiko baldintzentzat, jarraitzen saiatu ordez, akats bat gertatzeko.

Azkenik, [CVE-2024-0743](#) kalteberatasunak Firefox ESRren 115.9 bertsioaren aurreko bertsioei eta Thunderbirdko bezeroaren 115.9 bertsioaren aurreko bertsioei eragiten die. Kalteberatasunaren jatorria da TLSren estekaren protokolo-kodean dagoen egiaztatu gabeko itzulketa-balioa. Horrek ustua daitekeen blokea eragin dezake.

#### 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.

Arazo horiek konpontzeko, Mozillak Firefoxen bertsiorik berriena instalatzea gomendatzen du. Nabigatzailea eguneratzeko jarraibideak [esteka honetan](#) daude.

Mozilla Thunderbirden kasuan, eguneratze-jarraibideak [esteka honetan](#) kontsulta litezke.

## 5. Erreferentzia gehigarriak

---

- CVE-2024-2615.
- CVE-2024-2605.
- CVE-2024-2606.
- CVE-2024-2607.
- CVE-2024-2608.
- CVE-2024-2614.
- CVE-2024-2616.
- CVE-2024-0743.



