



Google Chromen kalteberatasunak

CYBERZAINITZA-ABISUAK

TLP: CLEAR

www.zibersegurtasun.eus



EUSKO JAURLARITZA
GOBIERNO VASCO

EDUKI-TAULA

1. Resumen ejecutivo.....	3
2. Recursos afectados	4
3. Análisis técnico	5
4. Mitigación / Solución.....	7
5. Referencias Adicionales	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 etorrita, 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

Googlek [segurtasun-abisuak](#) argitaratu ditu. Batetik, LTS kanala eguneratu du **ChromeOS**-erako, eta larritasun handiko **2 kalteberatasun** zuzendu ditu. Hona hemen horien identifikatzaileak: [CVE-2024-0225](#) eta [CVE-2024-1059](#). Kalteberatasun horiek [Use-After-Free](#) baldintzak sortzen dituzte **WebGPU** eta **WebRTC** softwareetan.

Bestetik, kanal egonkorra zuzendu zaie Windows eta Mac-erako 122.0.6261.111/.112 bertsioari eta Linuxerako 122.0.6261.111 bertsioari. Horietan **larritasun handiko 3 kalteberatasun** zuzendu dituzte, honako identifikatzaileak dituztenak: [CVE-2024-2173](#), [CVE-2024-2174](#) eta [CVE-2024-2176](#).

Gainera, hirugarrenen segurtasunerako soluzioak ere gehitu dira; esaterako, [CVE-2024-0646](#) akatsa zuzendu da Linuxeko kernelean.

Googleren segurtasun-politika dela eta, ez da kalteberatasun horietako batzuen informazio zehatzik eman, haien ustiapena saihesteko. Hori dela eta, espezifikazio teknikoek mugatuta jarrai dezakete erabiltzaile gehienek Googlek eskainitako segurtasun-eguneratzeak aplikatu arte.

2. Kaltetutako baliabideak

- Chrome OSerako epe luzeko asistentzia-kanala, LTS-114.0.5735.355en aurreko bertsioetan (plataforma: 15437.95.0).
- Google Chrome, 121.0.6167.139 baino lehenagoko bertsioak.
- Windows eta Macerako kanal egonkorra, 122.0.6261.111/.112 baino lehenagoko bertsioetan.
- Linuxerako kanal egonkorra, 122.0.6261.111 baino lehenagoko bertsioetan.

3. Azterketa tekniko

Abisu honetan landutako kalteberatasunen xehetasunak hauek dira:

CVE-2024-0225: [Use-After-Free](#) kalteberatasuna WebGPUn, 120.0.6099.199 baino lehenagoko Google Chromen. Urruneko erasotzaile bati Heaparen korrupzioa potentzialki ustiatzeko aukera ematen dio, berak sortutako HTML orrialde baten bidez.

Kalteberatasunen azterketaren neurketak honako hauek ditu:

CWE-416: Erabili After Free

Oinarrizko CVSSa: **8.8**

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

- **Eraso-bektorea: Sarea**
- **Erasoaren konplexutasuna: Baxua**
- **Beharrezko pribilegioak: Bat ere ez**
- **Interakzioa erabiltzailearekin: Beharrezkoa**
- **Aplikazio-eremua: Aldaketarik gabe**
- **Konfidentzialtasuna: Altua**
- **Integritatea: Altua**
- **Eskuragarritasuna: Altua**

CVE-2024-1059: [Use-After-Free](#) kalteberatasuna Peer Connectionen, 121.0.6167.139 baino lehenagoko Google Chromen. Urruneko erasotzaile bati Heaparen korrupzioa potentzialki ustiatzeko aukera ematen dio, berak sortutako HTML orrialde baten bidez.

Kalteberatasunen azterketaren neurketak honako hauek ditu:

CWE-416: Erabili After Free

Oinarrizko CVSSa: **8.8**

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

- **Eraso-bektorea: Sarea**
- **Erasoaren konplexutasuna: Baxua**
- **Beharrezko pribilegioak: Bat ere ez**
- **Interakzioa erabiltzailearekin: Beharrezkoa**
- **Aplikazio-eremua: Aldaketarik gabe**
- **Konfidentzialtasuna: Altua**
- **Integritatea: Altua**

- **Eskuragarritasuna: Altua**

[CVE-2024-0646](#): mugetatik kanpo memoria idaztean datzan kalteberatasuna, Linuxeko kernelaren garraio-geruzaren segurtasun-funtzionalitatean, erabiltzaileak splice funtzio bati dei egiten dionean, socket ktls bat helburu duela. Akats horrek baimena ematen dio tokiko erabiltzaile bati blokeo bat eragiteko, edo sisteman dituen pribilegioak areagotzeko.

Kalteberatasunen azterketaren neurketak honako hauek ditu:

[CWE 787](#): Out-of-bounds Write

Oinarritzko CVSSa: **7.8**

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

- **Eraso-bektorea**: Bertakoa
- **Erasoaren konplexutasuna**: Baxua
- **Beharrezko pribilegioak**: Baxuak
- **Interakzioa erabiltzailearekin**: Bat ere ez
- **Aplikazio-eremua**: Aldaketarik gabe
- **Konfidentzialtasuna**: Altua
- **Integritatea**: Altua
- **Eskuragarritasuna**: Altua

[CVE-2024-2173](#): mugetatik kanpo memoriara sartzeko kalteberatasuna V8n.

[CVE-2024-2174](#): ezarpen desegokiaren kalteberatasuna V8n.

[CVE-2024-2176](#): [Use-After-Free](#) kalteberatasuna FedCMn

4. Arintzea / Konponbidea

Kalteberatasun horiek arintzeko, sistemak eta aplikazioak beti eskuragarri dagoen azken bertsioarekin eguneratzea gomendatzen da, argitaratu bezain laster.

Horretarako, Windowserako, Macerako eta Linuxerako kanal egonkorra eguneratu behar da. Chromen ekite-kanalak eguneratzeko segurtasun-irtenbide ofiziala [esteka honetan](#) dago.

Azkenik, LTS kanala 114.0.5735.355 bertsiora eguneratu beharko da (plataforma-bertsioa: 15437.95.0). Google Chrome eguneratzeko, segurtasun-konponbide ofiziala eskuz jaits daiteke esteka honen bidez:

- [Google Chromeren Windowserako, Macerako eta Linuxerako eguneratzea](#).

5. Erreferentzia gehigarriak

- [Segurtasun-abisua.](#)
- [CVE-2024-0225.](#)
- [CVE-2024-1059.](#)
- [CVE-2024-0646.](#)
- [CVE-2024-2173.](#)
- [CVE-2024-2174.](#)
- [CVE-2024-2176.](#)

