



Larritasun handiko kalteberatsunak Google Chromen

CYBERZAINITZA-ABISUAK

TLP: CLEAR

www.zibersegurtasun.eus



EDUKI-TAULA

1. Laburpen exekutiboa	3
2. Kaltetutako baliabideak.....	4
3. Azterketa teknikoa.....	5
4. Murriztea / Konponbidea.....	6
5. Erreferentzia gehigarriak	7

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 erantzuleztat, ezta kanpoko web-orrialdeetarako esteka bidez sartutako bestelako informazioaren, software produktuen edo Zibersegurtasunaren Euskal Agentziaren webgunean edo alertan ager daitezkeen beste edozein informazioaren erantzuleztat 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-abisua](#) igorri du Mac-erako eta Linuxerako 121.0.6167.160 kanal egonkorra eguneratzeko eta Windowserako 121.0.6167.160/161 kanala eguneratzeko. Hurrengo egunetan/asteetan jarriko da martxan, bertan **larritasun handiko 2 kalteberatasun** zuzentzen dira, [CVE-2024-1284](#), [CVE-2024-1283](#) identifikatzaileak dituztenak.

Googleren segurtasun-politika dela eta, momentuz ez da kalteberatasun horien 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

- Mac-erako 121.0.6167.160 bertsioa baino lehenagokoetako kanal egonkorra.
- Linuxen eta Windowsen 121.0.6167.160/161 bertsioa baino lehenagokoetarako kanal egonkorra.

3. Azterketa teknikoa

Abisu honetan landutako kalteberatasunen xehetasunak hauek dira:

[CVE-2024-1284](#): Use-After-Free ahultasuna Mojo sisteman.

[CVE-2024-1283](#): Heap bufferra gainezkatzeko kalteberatasuna Skia-n.

4. Murriztea / Konponbidea

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

Google Chrome eguneratzeko, segurtasun-konponbide ofiziala eskuz jaits daiteke esteka honen bidez:

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

5. Erreferentzia gehigarriak

- Segurtasun-abisua.
- CVE-2024-1284.
- CVE-2024-1283.

