cyber zaintza
BASQUE CYBERSECURITY AGENCY

Larritasun handiko kalteberatsunak Google Chromen

CYBERZAINTZA-ABISUAK

TLP: CLEAR

www.zibersegurtasun.eus

EUSKO JAURLARITZA
GOBIERNO VASCO

EDUKI-TAULA

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

1. Laburpen exekutiboa

Googlek segurtasun-abisua igorri du Mac-erako eta Linuxerako 121.0.6167.139 kanal egonkorra eguneratzeko eta Windowserako 121.0.6167.139/140 kanala eguneratzeko. Hurrengo egunetan/asteetan jarriko da martxan, bertan **4 kalteberatasun** zuzentzen dira, horietatik 3 **larritasun handikoak** dira CVE-2024-1060, CVE-2024-1059, CVE-2024-1077 identifikatzaileak dituztenak.

Googleren segurtasun-politika dela eta, momentuz 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

- Mac eta Linuxerako 121.0.6167.139 bertsioa baino lehenagokoetako kanal egonkorra.
- Windowsen 121.0.6167.139/140 bertsioa baino lehenagokoetarako kanal egonkorra.

3. Azterketa teknikoa

Abisu honetan landutako kalteberatasunen xehetasunak hauek dira:

CVE-2024-1060: Use-After-Free kalteberatasuna Canvas-en 121.0.6167.139 bertsioa baino lehenagoko Google Chromen. Kalteberatasun horrek urruneko erasotzaileari HTML orrialde baten bidez heaparen korrupzioa potentzialki ustiatzeko aukera ematen zion.

CVE-2024-1059: Use-After-Free kalteberatasuna 121.0.6167.139 baino lehenagoko Google Chromen. Urruneko erasotzaileari diseinatutako HTML orrialde baten bidez pilaren korrupzioa ustiatzeko aukera ematen zion.

CVE-2024-1077: Use-After-Free kalteberatasuna 121.0.6167.139 baino lehenagoko Google Chromen. Urruneko erasotzaileari fitxategi maltzur baten bidez heaparen korrupzioa ustiatzeko aukera ematen zion.

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-2024-1060
- CVE-2024-1059
- CVE-2024-1077


cyber
zaintza
BASQUE CYBERSECURITY AGENCY