Basque CyberSecurity Centre

Ahultasunak ChromeOS-en

TLP: CLEAR

www.zibersegurtasun.eus

EUSKO JAURLARITZA
GOBIERNO VASCO

GRUPO spri TALDEA

AURKIBIDEA

Erantzukizunetik salbuesteari buruzko klausula

Honako dokumentu hau eskaintzen da erakundeen eta interesa duten herritarren segurtasunerako BCSCk beharrezkotzat jotzen dituen alertak ezagutzera emateko. Inongo kasutan BCSC ezin da kontsideratu hemen zabaldutako informazioaren erabilpenak zuzenean nahiz zeharka, ustekabean nahiz modu berezian, eragin litzakeen balizko kalteen arduradun. Gauza bera esan beharra dago BCSCren webean edo hortik esteken bitartez joan litekeen kanpoko web orrialdeetan, sare sozialetan, software produktuetan edo alertan nahiz BCSCren webean agertutako beste edozein informaziotan aipa litezkeen teknologiei dagokienez. Edozein kasutan, alertaren edukiak eta mezu elektronikoen bidez eman litezkeen erantzunak hemen jasotako terminoetan emandako iritzi eta gomendioak dira eta jakinarazitako informaziotik ezin da ondorioztatu ondorio juridiko loteslerik.

Salmenta debekatzeari buruzko klausula

BCSCri buruz

Zibersegurtasun Euskal Zentroa (Basque Cybersecurity Centre, BCSC) da Eusko Jaurlaritzak izendatutako entitatea Euskadin zibersegurtasunaren gaian heldutasun maila igotzeko.

Zeharkako ekimena da, Enpresa Garapenerako Euskal Agentziaren (SPRI) barnean kokatua, Eusko Jaurlaritzako Ekonomiaren Garapen, Jasangarritasun eta Ingurumen Sailaren menpe dagoen sozietatea. Segurtasuna, Gobernantza Publiko eta Autogobernua, eta Hezkuntza, bai eta Zientzia, Teknologia eta Berrikuntzako Euskal Sareko eragile ezberdinak ere. Tecnalia, Vicomtech, Ikerlan eta BCAM.

BCSC erreferentziazko entitatea da zibersegurtasuna eta konfiantza digitala garatzeko Euskadiko herritar, enpresa eta instituzio publikoen artean, eta batez ere, eskualdeko ekonomiaren sektore estrategikoen kasuan.

Beraz, BCSCren eginkizuna da euskal gizartean zibersegurtasuna sustatzea eta garatzea, Euskadiko enpresa jarduera dinamizatzea eta erreferentzia izango den sektore profesional bat sor dadin eragitea. Testuinguru horretan osagarriak diren eragileen arteko lankidetza proiektuak exekutatzea sustatzen du, berrikuntza teknologikoaren, ikerkuntzaren, eta fabrikazio aurreratuko industriarako eta beste sektore batzuetarako transferentzia teknologikoaren alorretan.

Era berean, hainbat zerbitzu eskaintzen ditu Gertakarien Aurreko Ekipo modura duen rolagatik (aurrerantzean CERT, ingelesezko izenaren siglak direla-eta “Computer Emergency Response Team”). Euskal Autonomia Erkidegoko esparruan mehatxu berriak antzemateko eta horiei buruzko alerta goiztiarrak emateko gaitasuna areagotzen dihardu lanean, informazioaren segurtasun gertakarien erantzunean eta analisian, eta euskal gizartearen beharrak artatzeko beharrezkoak diren prebentzio neurrien diseinuan. Helburu horiek lortzeko xedearekin, zibersegurtasun gertakariak kudeatzera zuzendutako hainbat ekimenetan hartzen du parte:

FIRST Improving Security Together
TF-CSIRT Trusted Introducer
CSIRT.es

1. Laburpen exekutiboa

Googlek segurtasun ohar bat argitaratu du, ChromeOS-rako laguntza kanalaren eguneraketa iragarriz. ChormeOS-rako laguntza kanalak guztira 3 akats jasotzen ditu. Hirurak kalifikatu dira larritasun altu batekin, eta honako identifikatzaileekin erregistratuak izan dira: CVE-2023-2135, CVE-2023-2134 eta CVE-2023-2133. Akats horiek guztiak arrakastaz ustiatuak izanez gero kaltetutako sistemen konfidentzialtasun, integritate eta eskuragarritasunean larritasun altuko inpaktua eragingo litzateke.

Fabrikatzaileak dagoeneko argitaratu ditu dagozkion eguneraketak, eta horien bitartez zuzendu egin dira nabarmendutako akatsak. Ahultasun hauek eta beste batzuk prebenitzeko gomendatzen da sistemak eta aplikazioak beti eguneratuta izatea eskuragarri dagoen azken bertsiora, dagozkion eguneraketak argitaratu bezain azkar.

2. Azterketa teknikoa

Eguneraketa honetan zuzendutako ahultasunen xehetasunak honako hauek dira:

CVE-2023-2134: memoriarako mugez kanpoko sarbide erako ahultasuna Service Worker-en APIan, Google Chromeren 112.0.5615.137 bertsioa baino lehenagokoetan. Hori baliatuz urruneko erasotzaile batek heap-aren hondatzea ustia lezake agian, manipulatutako HTML orrialde baten bidez.

Ahultasunaren ebaluazioaren metrika honela osatzen da:

CWE 787: Out-of-bounds Write

CVSS Base: 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**
- **Behar diren pribilegioak: Batere ez**
- **Erabiltzailearekiko interakzioa:** Beharrezkoa
- **Irismena:** Aldaketarik gabe
- **Konfidentzialtasuna: Altua**
- **Integritatea: Altua**
- **Eskuragarritasuna: Altua**

CVE-2023-2133: memoriarako mugez kanpoko sarbide erako ahultasuna Service Worker-en APIan, Google Chromeren 112.0.5615.137 bertsioa baino lehenagokoetan. Hori baliatuz urruneko erasotzaile batek heap-aren hondatzea ustia lezake agian, manipulatutako HTML orrialde baten bidez.

Ahultasunaren ebaluazioaren metrika honela osatzen da:

CWE 787: Out-of-bounds Write

CVSS Base: 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**
- **Behar diren pribilegioak: Batere ez**
- **Erabiltzailearekiko interakzioa:** Beharrezkoa
- **Irismena:** Aldaketarik gabe
- **Konfidentzialtasuna: Altua**
- **Integritatea: Altua**
- **Eskuragarritasuna: Altua**

CVE-2023-2135: Use-After-Free erako ahultasuna Google Chromeren DevTools-en, 112.0.5615.137 baino lehenagoko bertsioetan. Hori baliatuz urruneko erasotzaile batek erabiltzaile bat engaina lezake aldez aurreko baldintza

zehatzak gaitu ditzan eta horrela heap-aren hondatzea balia lezake agian, manipulatutako HTML orrialde baten bidez.

Ahultasunaren ebaluazioaren metrika honela osatzen da:

CWE 416: Use After Free

CVSS Base: 7.5

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

- **Eraso bektorea: Sarea**
- **Erasoaren konplexutasuna:** Altua
- **Behar diren pribilegioak: Batere ez**
- **Erabiltzailearekiko interakzioa:** Beharrezkoa
- **Irismena:** Aldaketarik gabe
- **Konfidentzialtasuna: Altua**
- **Integritatea: Altua**
- **Eskuragarritasuna: Altua**

Azkenik, aurreko ahultasunek eragindako produktuak honako hauek dira:

- ChromeOS gailu gehienen kasuan, LTS-108 108.0.5359.231 bertsiora eguneratzen ari da LTS kanalean, plataformaren 15183.94.0 bertsiorako.

3. Arintzea / Konponbidea

Ohikoa den moduan, ahultasun hau eta beste batzuk prebenitzeko gomendatzen da sistemak eta aplikazioak beti eguneratuta izatea eskuragarri dagoen azken bertsiora, dagozkion eguneraketak argitaratu bezain azkar.

ChromeOS sistemei dagokienez, 108.0.5359.231 bertsiora eguneratuak izan behar dira, ondorengo estekan azpimarratzen diren jarraibideen arabera:

- Chromebook-aren sistema eragilea nola eguneratu.

4. Erreferentzia Osagarriak

- Laguntza kanalaren eguneraketa.
- CVE-2023-2135.
- CVE-2023-2134.
- CVE-2023-2133.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA