Basque CyberSecurity Centre

Ahultasunak Google Chromen

BCSC-OHARRAK

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. Segurtasun oharra

Googlek segurtasun ohar bat argitaratu du, Google Chrome-ren 114 bertsiorako eguneraketa aztertzen duena, kanal egonkorraren barnean. Deskargatzeko eta erabilera orokorrerako erabilgarri dago. Ohar honetan guztira 16 akats zuzendu dira. Horien artetik 8 larritasun altukotzat sailkatu ditu enpresak, honako identifikatzaileak dituztenak hain zuzen: CVE-2023-2929, CVE-2023-2930, CVE-2023-2931, CVE-2023-2932, CVE-2023-2933, CVE-2023-2934, CVE-2023-2935, CVE-2023-2936.

Googleren segurtasun politika dela eta, oraingoz ahultasun honi buruzko xehetasunik ez da eman, bere ustiapena ekiditeko. Horregatik espezifikazio teknikoak murriztuta manten daitezke erabiltzaile gehienek Googlek eskainitako segurtasun eguneraketak ezarri arte.

2. Kaltetutako baliabideak

- Google Chrome, Linux eta Mac-erako 114.0.5735.90 bertsioa baino lehenagokoak.
- Google Chrome, Windowserako 114.0.5735.90/91 bertsioa baino lehenagokoak.

3. Azterketa teknikoa

Eguneraketa honetan aztertutako ahultasun garrantzitsuenen xehetasunak honakoak dira:

CVE-2023-2929: mugez kanpoko idazketa Swiftshader-en. Hori baliatuz urruneko erasotzaile batek heap-aren hondatzea balia lezake agian, manipulatutako HTML orrialde baten bidez.

CVE-2023-2930: Use-after-free erako ahultasuna Google Chrome-ren luzapenetan 114.0.5735.90 baino lehenagoko bertsioetan. Hori baliatuz erasotzaile batek erabiltzaile bat engaina lezake, asmo gaiztoko luzapen bat instala dezan heap-aren hondatzea ustiatzeko agian, manipulatutako HTML orrialde baten bidez.

CVE-2023-2931: Use-after-free erako ahultasuna PDFn Google Chrome-ren 114.0.5735.90 baino lehenagoko bertsioetan. Hori baliatuz urruneko erasotzaile batek heap-aren hondatzea balia lezake agian, manipulatutako PDF fitxategi baten bidez.

CVE-2023-2932: Use-after-free erako ahultasuna PDFn Google Chrome-ren 114.0.5735.90 baino lehenagoko bertsioetan. Hori baliatuz urruneko erasotzaile batek heap-aren hondatzea balia lezake agian, manipulatutako PDF fitxategi baten bidez.

CVE-2023-2933: Use-after-free erako ahultasuna PDFn Google Chrome-ren 114.0.5735.90 baino lehenagoko bertsioetan. Hori baliatuz urruneko erasotzaile batek heap-aren hondatzea balia lezake agian, manipulatutako PDF fitxategi baten bidez.

CVE-2023-2934: mugez kanpoko memoriarako sarbide erako ahultasuna Mojo-n Google Chrome-ren 114.0.5735.90 baino lehenagoko bertsioetan. Hori baliatuz urruneko erasotzaile batek heap-aren hondatzea balia lezake agian, manipulatutako HTML orrialde baten bidez.

CVE-2023-2935: moten nahasketa erako ahultasuna V8-n Google Chrome-ren 114.0.5735.90 baino lehenagoko bertsioetan. Hori baliatuz urruneko erasotzaile batek heap-aren hondatzea balia lezake agian, manipulatutako HTML orrialde baten bidez.

CVE-2023-2936: moten nahasketa erako ahultasuna V8-n Google Chrome-ren 114.0.5735.90 baino lehenagoko bertsioetan. Hori baliatuz urruneko erasotzaile batek heap-aren hondatzea balia lezake agian, manipulatutako HTML orrialde baten bidez.

4. Arintzea / Konponbidea

Ahultasun hauek arintzeko gomendatzen da sistemak eta aplikazioak beti eguneratuta izatea eskuragarri dagoen azken bertsiora, dagozkion eguneraketak argitaratu bezain azkar.

Horretarako Google Chrome Linux eta Mac-erako 114.0.5735.90 bertsiora egunera beharra dago eta Windows sistemetan 114.0.5735.90/91 bertsiora. Segurtasunezko konponbide ofiziala eskuz deskarga daiteke honako estekatik:

- Google Chromeren eguneraketa Windows, Mac eta Linuxerako.

Modu osagarrian, Googlek jarraibideak eskaini ditu Chrome bilatzailea modu zuzenean eguneratzeko pausoak azalduz. Informazio horretarako esteka honen bitartez irits daiteke:

- Google Chrome eguneratzeko jarraibideak.

5. Erreferentzia Osagarriak

- Segurtasun oharra.
- CVE-2023-2929.
- CVE-2023-2930.
- CVE-2023-2931.
- CVE-2023-2932.
- CVE-2023-2933.
- CVE-2023-2934.
- CVE-2023-2935.
- CVE-2023-2936.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA