Basque CyberSecurity Centre

Google Chromeren kalteberatasunak Chrome OS-en (CVE-2023-0128, CVE-2023-0137)

BCSC-ABISUAK

TLP: CLEAR

www.zibersegurtasun.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

EDUKIEN TAULA

Erantzukizunetik salbuesteko klausula

Dokumentu hau ematen da BCSCk erakundeen eta herritar interesdunen segurtasunaren alde beharrezkotzat jotzen dituen alertak zabaltzeko. BCSC ez da inola ere erantzule izango emandako informazioa erabiltzeak zuzenean edo zeharka, ustekabean edo ohiz kanpo eragin ditzakeen kalteen gainean, ez eta BCSCren webgunean aipatzen diren teknologiak edo kanpoko informazioa erabiltzeak eragin ditzakeen kalteen gainean ere, baldin eta kanpoko webguneetara, sare sozialetara, software-produktuetara edo alertan edo BCSCren webgunean ager daitekeen beste edozein informaziotara sartzeko estekak baditu. Alertaren edukiak eta mezu elektronikoen bidez eman daitezkeen erantzunak hemen jasotako baldintzen araberako iritzi eta gomendioak dira, eta ezin da jakinarazitako informaziotik ondorio juridiko loteslerik atera.

Salmenta debekatzeko klausula

BCSCri buruz

Zibersegurtasunaren Euskal Zentroa (Basque Cybersecurity Centre, BCSC) Eusko Jaurlaritzak Euskadiko zibersegurtasunaren heldutasun-maila areagotzeko izendatutako erakundea da.

Enpresa Garapenerako Euskal Agentziaren (SPRI) esparruko ekimen transbertsal bat da. Eusko Jaurlaritzako Ekonomiaren Garapen, Jasangarritasun eta Ingurumen Sailaren mendeko sozietate bat da berau. Eusko Jaurlaritzako beste hiru sailekin ere badu harremana: Segurtasun Sailarekin, Gobernantza Publiko eta Autogobernu Sailarekin eta Hezkuntza Sailarekin. Horrez gain, Zientzia, Teknologia eta Berrikuntzaren Euskal Sareko lau eragilerekin ere bai: Tecnalia, Vicomtech, Ikerlan eta BCAM.

BCSC erreferentziako erakundea da Euskadin herritarren, enpresen eta erakunde publikoen zibersegurtasuna eta konfiantza digitala garatzeari dagokionez; batez ere, eskualdeko ekonomian estrategikoak diren sektoreentzat.

BCSCren egitekoa, beraz, euskal gizartean zibersegurtasuna sustatzea eta garatzea da, Euskadiko enpresa-jarduera dinamizatzea, eta erreferente izango den sektore profesional bat sortzea. Testuinguru horretan, berrikuntza teknologikoaren, ikerketaren eta fabrikazio aurreratuko industriara eta beste sektore batzuetara transferentzia teknologikoa egiteko arloetan elkarren osagarri diren eragileen artean lankidetza-proiektuak gauzatzea bultzatzen da.

Era berean, zenbait zerbitzu eskaintzen ditu Gorabeherei Erantzuteko Talde gisa duen rolean (aurrerantzean, CERT, ingelesezko “Computer Emergency Response Team” siglen arabera), eta eginkizun hauek betez aritzen da lanean Euskal Autonomia Erkidegoan: mehatxu berriak detektatzeko eta garaiz ohartarazteko gaitasuna handituz, informazioaren segurtasuneko gorabeherei erantzunez eta horiek analizatuz, eta euskal gizartearen beharrei erantzuteko prebentzio-neurriak diseinatuz. Helburu horiek lortzeko asmoz, zibersegurtasun-gorabeherak kudeatzera bideratutako hainbat ekimenetan hartzen du parte:

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

1. Segurtasun-oharra

Googlek segurtasun-ohar berri bat argitaratu zuen joan den 2023ko urtarrilaren 13an, Chrome OS sistema eragileari eta Google Chrome nabigatzaileari eragiten dieten 2 hutsune konpontzeko. Kalteberatasunak, CVE-2023-0128 eta CVE-2023-0137 identifikatzaileak dituztenak, use-after-free eta Out-of-bounds Write motakoak dira, hurrenez hurren, eta larritasun handiarekin katalogatuta daude.

Kalteberatasun horiek ustiatu ahal izateko, erasotzaileek biktimak engainatu behar dituzte gizarte-ingeniaritzako tekniken bidez, eta inpaktu handia eragiten dute eragindako sistemen konfidentzialtasunean, osotasunean eta erabilgarritasunean.

2. Eragindako baliabideak

- Google Chromeko azalpen orokorreko modua (Overview Mode) Chrome OS-en 109.0.5414.74 baino lehenagoko bertsioan
- Google Chromeko aplikazioen plataforma Chrome OS-en 109.0.5414.74 baino lehenagoko bertsioan

3. Analisi teknikoa

Hona hemen tratatutako kalteberatasunen xehetasunak:

CVE-2023-0128: use-after-free kalteberatasuna Google Chromeko azalpen orokorreko moduan, 109.0.5414.74 baino lehenagoko Chrome OS-en. Urruneko erasotzaile bati aukera ematen dio erabiltzaile bat engainatzeko erabiltzaile-interfazean interakzio espezifikoak egin ditzan, HTML orri manipulatu baten bidez heap-aren hondatzea ustiatzeko.

Kalteberatasuna ebaluatzeko metrika honako hau da:

CVSS Base: 8.8, handia

CWE 416: Use After Free

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

- **Eraso-bektorea: Sarea**
- **Erasoaren konplexutasuna: Txikia**
- **Eskatutako pribilegioak: Bat ere ez**
- **Erabiltzailearekiko interakzioa**: Beharrezkoa
- **Irismena:** Aldaketarik gabe
- **Konfidentzialtasuna: Handia**
- **Osotasuna: Handia**
- **Erabilgarritasuna: Handia**

CVE-2023-0137: heap-aren bufer-gainezkatzearen kalteberatasuna Google Chrome-ko plataformako aplikazioetan 109.0.5414.74 baino lehenagoko Chrome OS-en; erasotzaile bati aukera ematen dio erabiltzaile bat engainatzeko hedapen gaizto bat instala dezan HTML orri manipulatu baten bidez heap-aren hondatzea ustiatzeko.

Kalteberatasuna ebaluatzeko metrika honako hau da:

CVSS Base: 8.8, handia

CWE 787: Out-of-bounds Write

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

- **Eraso-bektorea: Sarea**
- **Erasoaren konplexutasuna: Txikia**
- **Eskatutako pribilegioak: Bat ere ez**
- **Erabiltzailearekiko interakzioa**: Beharrezkoa
- **Irismena:** Aldaketarik gabe
- **Konfidentzialtasuna: Handia**
- **Osotasuna: Handia**
- **Erabilgarritasuna: Handia**

4. Arintzea / Konponbidea

Kalteberatasunak arintzeko, hauxe gomendatzen du BCSCk: dagozkion eguneraketak argitaratu bezain laster, sistemak eta aplikazioak erabilgarri dagoen azken bertsiora eguneratuta edukitzea beti.

Hutsegite horiek konpontzeko, Googlek tresna bakoitzaren azken bertsio erabilgarrietara eguneratzea gomendatzen du.

5. Erreferentzia gehigarriak

- Googleren segurtasun-oharrak
- Use-after-free
- Out-of-bounds Write
- CVE-2023-0128
- CVE-2023-0137
- ChromeOS
- Google Chrome

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA