Basque CyberSecurity Centre

Firefox eta Firefox ESRren kalteberatasunak

BCSC-ABISUAK

TLP: CLEAR

www.zibersegurtasun.eus

EUSKO JAURLARITZA
GOBIERNO VASCO

GRUPO spri TALDEA

EDUKIAREN TAULA

BCSCri buruz 3
1. Segurtasun-oharra 4
2. Eragindako baliabideak 5
3. Analisi teknikoa 6
4. Arintzea / Konponbidea 7
5. Erreferentzia gehigarriak 8

Erantzukizunetik salbuesteko klausula

Erakundeen eta herritar interesdunen segurtasunaren mesedetan, BCSCk beharrezkotzat jotzen dituen alertak zabaltzeko helburua du honako dokumentu honek. 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

Mozilla Foundation-ek bi segurtasun-ohar argitaratu ditu Firefox eta Firefox ERS nabigatzaileetako hutsegiteak zuzentzeko. Firefox ERS korporazio handi, unibertsitate eta enpresetarako bertsioa da. Bi horiek larritasun handikoak direla kalifikatu du fabrikatzaileak, eta bertan tratatutako kalteberatasun nagusiak CVE-2022-46871, CVE-2023-23598, CVE-2023-23605, CVE-2023-23597 eta CVE-2023-23606 dira. Larritasun handia dute, eta jada erabilgarri dago arintzeko segurtasun-eguneraketa.

2. Eragindako baliabideak

- Firefox ESR 102.7
- Firefox 109

3. Analisi teknikoa

Eguneraketa honetan tratatutako kalteberatasun garrantzitsuenen xehetasunak hauek dira:

CVE-2022-46871: libusrsctp liburutegiari eragiten dion kalteberatasuna, ustiatu zitezkeen hutsegiteak zituena.

Kalteberatasuna ebaluatzeko metrika honela dago osatuta:

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: Txikia**
- **Eskatutako pribilegioak: Bat ere ez**
- **Erabiltzailearekiko interakzioa**: Beharrezkoa
- **Irismena:** Aldaketarik gabe
- **Konfidentzialtasuna: Handia**
- **Osotasuna: Handia**
- **Erabilgarritasuna: Handia**

CVE-2023-23598: datuak arrastatzeko testu soileko Firefoxen GTK kodearen erabilerari eragiten dion kalteberatasuna; horrela, GTK-k testu soileko MIME guztiak, fitxategien URLak dituztenak, arrastatuak balira bezala tratatzen ditu, eta webgune batek DataTransfer.setData dei baten bidez fitxategi bat modu arbitrarioan irakurtzea ahalbidetu dezake.

CVE-2023-23605: Firefox 108 eta Firefox ESR 102.6 bertsioetan dauden memoria-segurtasuneko erroreak. Errore horietako batzuek memoria hondatzearen ebidentzia erakutsi zuten, eta baliteke kode arbitrarioa exekutatzeko ustiatuak izana.

CVE-2023-23597: kalteberatasun honetan, arriskuan jarritako bigarren mailako web-prozesu batek web-segurtasunaren irekiera-murrizketak desgaitu ditzake, eta horrek bigarren mailako prozesu berri bat sortzea eragingo luke file://file testuinguruaren barruan. Prozesu berri hori berriro ustiatu ahal izango litzateke, eta horrek fitxategien irakurketa arbitrarioa ahalbidetuko luke.

CVE-2023-23606: Firefox 108 eta Firefox ESR 102.6 bertsioetan dauden memoria-segurtasuneko erroreak. Errore horietako batzuek memoria hondatzearen ebidentzia erakutsi zuten, eta baliteke kode arbitrarioa exekutatzeko ustiatuak izana.

4. Arintzea / Konponbidea

Kalteberatasun horiek arintzeko, gomendatzen da sistema eta aplikazioak erabilgarri dagoen azken bertsiora eguneratuta edukitzea beti, dagozkien eguneraketak argitaratu bezain laster.

Kasu honetan, hornitzaileak eguneraketa bat eman du jada, jakinarazitako hutsegiteak zuzentzeko.

5. Erreferentzia gehigarriak

- Mozilla Foundation
- Segurtasun-oharrak
- Firefox ERS
- CVE-2022-46871
- CVE-2023-23598
- CVE-2023-23605
- CVE-2023-23597
- CVE-2023-23606

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA