Basque CyberSecurity Centre

Ahultasun kritikoa Django-n

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

2023ko maiatzaren 3an segurtasun ohar batean argitaratutako ahultasun baten egoera eguneratu egin da, web garapenerako Django framework-ari eragiten diona. CVE-2023-31047 identifikatzailea duen ahultasuna formularioen baliozkotzean bypass erako akats kritiko bat da. Hori arrakastaz ustiatuz gero, kaltetutako sistemen konfidentzialtasun, integritate eta eskuragarritasunean eragin altua suposatuko luke.

Fabrikatzaileak dagoeneko argitaratu du nabarmendutako akatsa konpontzen duen konponbidea. Horregatik, ahultasun hau eta beste batzuk prebenitzeko gomendatzen da sistemak eta aplikazioak beti eguneratuta izatea eskuragarri dagoen azken bertsiora.

2. Kaltetutako baliabideak

- Django 3.2, 3.2.19 bertsioa baino lehenagokoak.
- Django 4.0, 4.1.9 bertsioa baino lehenagokoak.
- Django 4.2, 4.2.1 bertsioa baino lehenagokoak.

3. Azterketa teknikoa

Eguneraketa honetan aztertutako ahultasunaren xehetasuna honakoa da:

CVE-2023-31047: formularioen baliozkotzean bypass erako ahultasuna. Hori dela eta, formulario baten eremu bat erabiliz hainbat fitxategi kargatzea ez da bateragarria *forms.FileField* edo *Forms.ImageField*-ekin, kargatutako azken fitxategia soilik baliozkotzen baita. Errorea saihesteko, formularioko *ClearableFileInput* eta *FileInput* widgetek orain *ValueError* bat sortzen dute beroietan HTML atributu anizkun bat ezartzen denean. Salbuespena ekiditeko eta lehenagoko portaera mantentzeko gomendatzen da *allow_multiple_selected* True balioan jartzea.

Ahultasunaren ebaluazioaren metrika honela osatzen da:

CWE 20: Improper Input Validation

CVSS Base: 9.8

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

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

4. Arintzea / Konponbidea

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

Azaldutako ahultasuna konpontzeko Djangok framework-erako eguneraketak argitaratu ditu, ondorengo esteketan eskuragarri daudenak:

- Django 4.2rako arintzea.
- Django 4.1rako arintzea.
- Django 3.2rako arintzea.

5. Erreferentzia Osagarriak

- Segurtasun oharra.
- CVE-2023-31047.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA