Basque CyberSecurity Centre

Ahultasun kritikoa GitLab Community Edition-en (CE) eta Enterprise Edition-en (EE)

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

BCSC-ri 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. Era berean, Eusko Jaurlaritzako beste hiru Sail ere bere parte dira: Segurtasuna, Gobernantza Publiko eta Autogobernua, eta Hezkuntza; bai eta Zientzia, Teknologia eta Berrikuntzako Euskal Sistemako lau eragile 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, ingeleseko 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

GitLabek segurtasun eguneratze bat argitaratu du. Bertan, ahultasun bati heltzen zaio, zeinaren larritasuna kritikotzat jo baita, eta Git biltegiak kokatzeko erabilitako kode irekiaren aplikazioari eragiten dio, GitLab Community Edition (CE) izenez ezagutzen denari. Era berean, GitLab Enterprise Edition (EE), Javan idatzitako aplikazioen softwarea garatzeko eta exekutatzeko programazio-plataforma, kaltebera da akats nabarmenaren aurrean.

Ahultasuna, CVE-2023-2825aren arabera identifikatua, oraingoz ez dago NISTren arabera CVSSv3 eskalaren araberako puntuaziorik esleituta, baina fabrikatzaileak kritikotzat jo du. Nabarmentzekoa da oraingoz ez dakigula akatsa sarean aktiboki ustiatzen ari denik.

Akats hori, pwnie ikertzaileak jakinarazia, zerbitzarian aurkitutako fitxategien irakurketa baten emaitza izan daiteke. Kalteberatasun nabarmenaren ustiapenak izan ditzakeen ondorio larrien arabera, irtenbidea da GitLabek emandako arintze-jarraibideak betetzea.

Fabrikatzaileak dagoeneko argitaratu du dagokion adabakia, eta, horrela, akats kritiko nabarmena zuzendu du. Beraz, urrakortasun hori eta beste batzuk prebenitzeko, sistemak eta aplikazioak eskuragarri dagoen azken bertsioan eguneratuta izatea gomendatzen da, dagozkion adabakiak argitaratu bezain laster.

2. Azterketa teknikoa

Ahultasun nabarmena CVE-2023-2825-ren bidez identifikatu zen, eta GitLab Community Edition (CE) eta GitLab Enterprise Edition (EE) eragiten die. Zehazkiago, aipatutako akatsak aukera ematen du direktorioak lekualdatzeko erasoak urrutitik egiteko. Ahultasuna gertatu da sarrera baliozkotzean errore bat gertatu delako, proiektu publiko batean fitxategi erantsi bat baldin badago eta gutxienez bost talde desberdinetan eskuragarri badago. Mehatxu aktore batek behar bezala ustiatzen badu, zerbitzarian dauden fitxategiak irakur ditzake.

Lehen deskribatutako ahultasuna ebaluatzeko metrikak honela osatzen dira:

CVSS Oinarria: 10.0

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

- **Eraso bektorea: Sarea**
- **Erasoaren konplexutasuna: Txikia**
- **Eskatutako pribilegioak: Bat ere ez**
- **Erabiltzailearekiko interakzioa: Bat ere ez**
- **Irismena: Aldaketekin**
- **Konfidentzialtasuna: Altua**
- **Osotasuna: Altua**
- **Erabilgarritasuna: Altua**

Azkenik, ahultasun horrek produktu hauei eragiten die:

- GitLab Community Edition (CE) 16.0.0. bertsioa
- GitLab Enterprise Edition (EE) 16.0.0. bertsioa

3. Arintzea / Konponbidea

Ohiko moduan, ahultasun horiei eta beste batzuei aurrea hartzeko, sistemak eta aplikazioak eskuragarri dagoen azken bertsiora eguneratuta izatea gomendatzen da, eguneratzeak argitaratu bezain laster.

Oso garrantzitsua da akatsak konpontzeko neurriak azkar hartzea. Horregatik, ahultasunaren larritasuna dela eta, enpresak emandako eguneratzeak 16.0.1 bertsioari aplikatzea gomendatzen da, GitLab Community Edition (CE) eta GitLab Enterprise Edition (EE) eguneratuz.

Eguneratze horiek lotura honen bidez aurki daitezke:

- https://about.gitlab.com/update/

Ahultasun hori larria denez, GitLab-en taldeak erabiltzaileei gomendatzen die ahalik eta azkarren egin dezatela produktu horien eguneratzea.

4. Erreferentzia osagarriak

- GitLab.
- GitLab Critical Security Release: 16.0.1.
- GitLab Community Edition (CE).
- GitLab Enterprise Edition (EE).
- Java.
- CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal').
- CWE-20: Improper Input Validation.
- Update GitLab.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA