Basque CyberSecurity Centre

Larritasun altuko ahultasuna Samba-n

BCSC-OHARRAK

TLP: CLEAR

www.zibersegurtasun.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

AURKIBIDEA

BCSCri buruz 3
1. Segurtasun oharra 4
2. Kaltetutako baliabideak 5
3. Azterketa teknikoa 6
4. Arintzea / Konponbidea 7
5. Erreferentzia Osagarriak 8

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

Sambak segurtasun ohar bat argitaratu du, CVE-2023-0614 identifikatzaile duen larritasun altuko ahultasun bat aztertzeko. Samba softwarearen 4.0 bertsioan eta geroagoko bertsio guztietan aurkitzen da.

Ahultasunaren berri lehenago ere eman zen, Sambaren 4.6.16, 4.7.9, 4.8.4 eta 4.9.7 bertsioetan aurkitu zen eta CVE-2018-10919 identifikatzailea eman zitzaion. Ustez zuzenduta zegoen, baina zuzenketa hura ez zela aski izan ikusi da. Izan ere, akatsak oraindik ahalbidetzen du erasotzaile batek Sambaren Active Directory (AD) domeinuaren kontrolatzaile baten BitLocker-en berreskuratze gako konfidentzialak eskuratzea. Ahultasun hori arrakastaz baliatuz gero kaltetutako sistemen konfidentzialtasunean inpaktu handia eragingo litzateke.

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

- Samba softwarearen bertsio guztiak, 4.0 bertsiotik aurrera.

3. Azterketa teknikoa

CVE-2023-0614: 4.0 bertsiotik aurrerako Sambaren bertsio guztietan, erasotzaile batek LDAPren bitartez BitLocker konfidentzialen berreskuratze gakoak eskuratzea ahalbidetzen duen ahultasuna. Ahultasuna existitzen da CVE-2018-10919 ahultasunerako aski izan ez zen partxe batengatik. Horrela urruneko erabiltzaile batek ezarrita dauden segurtasun murrizpenak saihets litzake eta informazio konfidentzialera sarbidea lortu.

Ahultasunaren ebaluazioaren metrika honela osatzen da:

CVSS Oinarrizkoa: 7.7

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

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

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, Sambak segurtasun eguneraketa bat argitaratu du, hemen eskuragarri:

- https://www.samba.org/samba/history/security.html

Era berean, ohar beraren barnean ahultasunak eragindako atributuen zerrenda eskaini da.

Modu osagarrian Sambaren erabiltzaileei gomendatzen zaie beren softwarea eguneratzea eta neurriak hartzea ziurtatzeko atributu konfidentzialetatik filtratuak izan ahal izan ziren datuak dagoeneko ez direla baliagarriak. Honek suposa dezake BitLocker-ekin enkriptatutako unitateak berriz enkriptatzea, TPM pasahitzak aldatzea eta Credential Roaming-ekin biltegiratzen diren ziurtagiriak baliogabetzea eta birjaulkitzea (gako sekretu berriekin).

Azkenik arazoa zuzentzeko Samba *$VERSIONS*-en segurtasun bertsioak argitaratu dira. Sambaren administratzaileei aholkatzen zaie bertsio horietara eguneratzea edo partxea lehenbailehen aplikatzea.

5. Erreferentzia Osagarriak

- Segurtasun oharra.
- CVE-2023-0614.
- CVE-2018-10919.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA