Basque CyberSecurity Centre

Ahultasunak Aruba ClearPass Policy Manager-en

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

El 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

Arubak, hainbat Segurtasun soluziorekin lotutako konpainiak, 8 ahultasun biltzen dituen ohar bat argitaratu du. Horien artean, ahultasun bat nabarmentzen da, fabrikatzaileak kritikotzat jo duena. Gainera, guztira 4 akats ditu, eta horiei larritasun handia eman zaie.

Ahultasuna, zeinaren larritasuna kritikotzat jo baita, honako identifikatzaile honen pean erregistratu da:

- CVE-2023-25589: sistemaren erabateko konpromisoan sor daitekeen ahultasuna.

Zorroztasun handiz katalogatu diren akatsei dagokienez, honako identifikatzaile hauetan erregistratu dira:

- CVE-2023-25590: Linux sistema eragileetan ClearPass OnGuarden pribilegioak tokian-tokian handitzea eragin dezaketen ahultasuna.
- CVE-2023-25591: ClearPass Policy Managerraren web kudeaketako interfazean informazioa zabaltzean gerta daitekeen ahultasuna.
- CVE-2023-25592 eta CVE-2023-25593: ClearPass Policy Managerraren web kudeaketako interfazean reflected cross site scripting (XSS) erasoa eragin dezaketen ahultasunak.

Fabrikatzaileak dagoeneko argitaratu ditu dagozkion adabakiak, eta, horrela, akats nabarmenak zuzendu ditu. Beraz, kalteberatasun horiek eta beste batzuk prebenitzeko, BCSCk sistema eta aplikazioak eskuragarri dagoen azken bertsioan eguneratuta izatea gomendatzen du, dagozkion adabakiak argitaratu bezain laster.

2. Azterketa teknikoa

Arubak emandako ahultasun kritikoari dagokionez, CVE-2023-25589an erregistratutako akatsa identifikatu da. Akats hori Daniel Jensen ikertzaileak jakinarazi du, ClearPass Policy Managerraren web kudeaketako interfazean erabiltzaile arbitrario bat sortzeko aukera dagoelako. Urruneko erasotzaile batek, sortutako erabiltzailearen bidez, helmugako sistemaren klusterra erabat arriskuan jar dezake.

Lehen deskribatutako ahultasuna ebaluatzeko metrikak honela osatzen dira:

CVSS Oinarria: 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: Txikia.**
- **Beharrezko pribilegioak: Bat ere ez.**
- **Erabiltzailearekiko interakzioa: Bat ere ez.**
- **Irismena: Aldaketarik ez.**
- **Konfidentzialtasuna: Altua.**
- **Osotasuna: Altua.**
- **Erabilgarritasuna: Altua.**

Larritasun handiko ahultasunari dagokienez, lehenengoa CVE-2023-25590, Luke Young ikertzaileak eman du horren berri. Akats hori ClearPass OnGuarden Linux sistema eragileetan pribilegioak modu lokalean eskalatzeko aukeragatik dago. Urruneko erasotzaile batek root pribilegioak dituen kode arbitrarioa exekutatu dezake helmugako sisteman.

Lehen deskribatutako kalteberatasuna ebaluatzeko metrikak honela osatzen dira:

CVSS Oinarria: 7.8

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

- **Eraso-bektorea: Lokala.**
- **Erasoaren konplexutasuna: txikia.**
- **Beharrezko pribilegioak: Txikia.**
- **Erabiltzailearekiko interakzioa: bat ere ez.**
- **Irismena: Aldaketarik ez.**
- **Konfidentzialtasuna: Altua.**
- **Osotasuna: Altua.**
- **Erabilgarritasuna: Altua.**

Era berean, CVE-2023-25591-ren barruan erregistratutako akatsa, larritasun handiz katalogatua eta Luke Young-ek emana, *ClearPass Policy Manager-en* web-kudeaketako interfazearen bidez eskura daitekeen informazio sentikorrerako pribilegio txikiak dituen erabiltzaile batek atzitzeko duen aukerak eragin du. Erasotzaile batek helmugako sisteman pribilegio gehigarriak lortzeko erabil daitezkeen datuak eskuratzeko aukera du.

Ahultasuna ebaluatzeko CVE-2023-25591 metrikak osagai hauek ditu:

CVSS Base: 7.6

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

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

Azkenik, CVE-2023-25592 eta CVE-2023-25593 erregistratutako akatsak oso kritikatuak izan dira. Hasieran, *Sicarius* ikertzaileak ahultasun horien berri eman du, erabiltzaileak *ClearPass Policy Manager-en* web-kudeaketako interfazearen barruan emandako datuak ez baitira behar bezala kudeatzen. Aktore maltzur batek HTML kodea injektatu eta exekuta dezake, baita script arbitrario bat ere eragindako interfazearen testuinguruan.

Aipatutako ahultasunak ebaluatzeko metrikak honela osatuta daude:

CVSS Base: 7.1

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

- **Eraso bektorea: Sarea**
- **Erasoaren konplexutasuna: Txikia.**
- **Beharrezko pribilegioak: Txikia.**
- **Erabiltzailearekiko interakzioa:** Beharrezkoa.
- **Irismena: Aldaketekin.**
- **Konfidentzialtasuna:** Txikia.
- **Osotasuna:** Txikia.
- **Erabilgarritasuna:** Txikia.

Azkenik, ahultasun horiek produktu hauei eragiten diete:

- *ClearPass Policy Manager* 6.11.1 bertsioa eta aurrekoak.
- *ClearPass Policy Manager* 6.10.8 bertsioa eta aurrekoak.
- *ClearPass Policy Manager* 6.9.13 bertsioa eta aurrekoak.

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.

Horretarako, *ClearPass Policy Manager* bertsio nabarmen hauetan eguneratu behar da:

- *ClearPass Policy Manager* 6.11.X: 6.11.2 bertsioa edo berriagoa eguneratu.
- *ClearPass Policy Manager* 6.10.X: 6.10.8 Hotfix 1 bertsioa edo berriagoa eguneratu.
- *ClearPass Policy Manager* 6.9.X: 6.9.13 Hotfix 1 bertsioa edo berriagoa eguneratu.

Horrez gain, Arubak Segurtasun neurri alternatiboen berri eman du. Neurri horiek arestian aipatutako irtenbideak ezarri ezin dituzten edo euskarritik kanpo dagoen bertsio bat duten administratzaileek aplikatu beharko dituzte.

Horretarako, Arubak gomendatzen du CLI kudeaketa interfazeak *ClearPass Policy Manager-en* web-orrian oinarritua 2. mailako segmentu/VLAN batera mugatzea, 3. geruzako edo hortik gorako firewall politiken bidez kontrolatua.

4. Erreferentzia osagarriak

- ARUBA-PSA-2023-003.
- ClearPass OnGuard Data Sheet.
- Aruba ClearPass Policy Manager Data Sheet.
- CWE-79: Improper neutralization of Input During Web Page Generation (‘Cross-site Scriptiing’).
- CWE-269: Improper Privilege Management.
- Daniel Jensen.
- Luke Young
- Aruba ClearPass Policy Manager 6.11 Online Help Portal.
- Aruba ClearPass Policy Manager 6.10 Online Help Portal.
- Aruba ClearPass Hardening Guide.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA