Basque CyberSecurity Centre

# Ahultasuna Aruba CX switch-etan

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

Arubak AOS-CX sistema eragilea exekutatzen duten switch kableatu jakin batzuetarako segurtasun eguneraketak argitaratu ditu. Horietan sarearen analisi motorrak (NAE) duen larritasun altuko ahultasun bat konpontzen da, CVE-2023-1168, identifikatzailea duena. Akatsak urruneko kode arbitrarioaren exekuzio egoera bat ekar dezake eta horrek inpaktu handia eragingo luke kaltetutako sistemen konfidentzialtasun, integritate eta eskuragarritasunean.

Nabarmendu beharra dago ohar hau argitaratzeko unean Arubaren arabera ez dela ezagutzen ahultasunaren hedapen publikorik edo ustiapen koderik.

## 2. Kaltetutako baliabideak

Aruba Switch modeloak:

- Aruba CX 10000 Switch Series.
- Aruba CX 9300 Switch Series.
- Aruba CX 8400 Switch Series.
- Aruba CX 8360 Switch Series.
- Aruba CX 8325 Switch Series.
- Aruba CX 8320 Switch Series.
- Aruba CX 6400 Switch Series.
- Aruba CX 6300 Switch Series.
- Aruba CX 6200F Switch Series.

Software bertsioak:

- AOS-CX 10.10.xxxx: 10.10.1020 eta beheragoko bertsioak.
- AOS-CX 10.09.xxxx: 10.09.1020 eta beheragoko bertsioak.
- AOS-CX 10.08.xxxx: 10.08.1070 eta beheragoko bertsioak.
- AOS-CX 10.06.xxxx: 10.06.0230 eta beheragoko bertsioak.

## 3. Azterketa teknikoa

Aztertutako ahultasunen xehetasunak honakoak dira:

CVE-2023-1168: AOS-CX sare analisiaren motorrari eragiten dion autentifikatutako urruneko kodearen exekuzio erako ahultasuna. Ahultasun hau arrakastaz baliatuz gero, azpiko sistema eragilean kode arbitrarioa exekuta liteke erabiltzaile pribilegiatu baten modura, eta horrek AOS-CX exekutatzen duen switch-a erabat jar dezake arriskuan.

Ahultasunaren ebaluazioaren metrika honela osatzen da:

CVSS Oinarrizkoa: 7.2

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

- **Eraso bektorea: Sarea**
- **Erasoaren konplexutasuna: Baxua**
- **Behar diren pribilegioak:** Altuak
- **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.

Oharrean azaldutako ahultasunari aurre egiteko, Arubak gomendazen du softwarea eguneratzea honako bertsio hauetako batera:

- AOS-CX 10.11.xxxx: 10.11.0001 eta goragokoa.
- AOS-CX 10.10.xxxx: 10.10.1030 eta goragokoa.
- AOS-CX 10.06.xxxx: 10.06.0240 eta goragokoa.

Arubak azpimarratu du ez direla ebaluatzen ezta eguneratzen ere zerbitzuaren amaierara iritsi diren AOS-CXren firmware bertsioak. Ohar hau argitaratzen den datan ondorengo hauek dira onartuta dauden bertsioak:

- AOS-CX 10.11.xxxx.
- AOS-CX 10.10.xxxx.
- AOS-CX 10.06.xxxx.

Azkenik, erasotzaile batek ahultasun hau baliatzeko aukerak murrizteko arintze neurri alternatibo modura, Arubak proposatzen du CLI-n eta webean oinarritutako kudeaketa interfazeak 2 geruzako dedikatutako segmentu/VLAN batera murriztea, edota 3. eta goragoko geruzetan firewall politikek kontrolatuak izatea.

## 5. Erreferentzia Osagarriak

- Segurtasun eguneraketa.
- CVE-2023-1168.


EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA