Basque CyberSecurity Centre

Kalteberatasunak - Aruba Orchestrator

BCSC-ABISUAK

TLP: CLEAR

www.zibersegurtasun.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

EDUKIEN TAULA

Erantzukizunetik salbuesteko klausula

Dokumentu hau ematen da BCSCk erakundeen eta herritar interesdunen segurtasunaren alde beharrezkotzat jotzen dituen alertak zabaltzeko. BCSC ez da inola ere erantzule izango emandako informazioa erabiltzeak zuzenean edo zeharka, ustekabean edo ohiz kanpo eragin ditzakeen kalteen gainean, ez eta BCSCren webgunean aipatzen diren teknologiak edo kanpoko informazioa erabiltzeak eragin ditzakeen kalteen gainean ere, baldin eta kanpoko webguneetara, sare sozialetara, software-produktuetara edo alertan edo BCSCren webgunean ager daitekeen beste edozein informaziotara sartzeko estekak baditu. Alertaren edukiak eta mezu elektronikoen bidez eman daitezkeen erantzunak hemen jasotako baldintzen araberako iritzi eta gomendioak dira, eta ezin da jakinarazitako informaziotik ondorio juridiko loteslerik atera.

Salmenta debekatzeko klausula

BCSCri buruz

Zibersegurtasunaren Euskal Zentroa (Basque Cybersecurity Centre, BCSC) Eusko Jaurlaritzak Euskadiko zibersegurtasunaren heldutasun-maila areagotzeko izendatutako erakundea da.

Enpresa Garapenerako Euskal Agentziaren (SPRI) esparruko ekimen transbertsal bat da. Eusko Jaurlaritzako Ekonomiaren Garapen, Jasangarritasun eta Ingurumen Sailaren mendeko sozietate bat da berau. Eusko Jaurlaritzako beste hiru sailekin ere badu harremana: Segurtasun Sailarekin, Gobernantza Publiko eta Autogobernu Sailarekin eta Hezkuntza Sailarekin. Horrez gain, Zientzia, Teknologia eta Berrikuntzaren Euskal Sareko lau eragilerekin ere bai: Tecnalia, Vicomtech, Ikerlan eta BCAM.

BCSC erreferentziako erakundea da Euskadin herritarren, enpresen eta erakunde publikoen zibersegurtasuna eta konfiantza digitala garatzeari dagokionez; batez ere, eskualdeko ekonomian estrategikoak diren sektoreentzat.

BCSCren egitekoa, beraz, euskal gizartean zibersegurtasuna sustatzea eta garatzea da, Euskadiko enpresa-jarduera dinamizatzea, eta erreferente izango den sektore profesional bat sortzea. Testuinguru horretan, berrikuntza teknologikoaren, ikerketaren eta fabrikazio aurreratuko industriara eta beste sektore batzuetara transferentzia teknologikoa egiteko arloetan elkarren osagarri diren eragileen artean lankidetza-proiektuak gauzatzea bultzatzen da.

Era berean, zenbait zerbitzu eskaintzen ditu Gorabeherei Erantzuteko Talde gisa duen rolean (aurrerantzean, CERT, ingelesezko “Computer Emergency Response Team” siglen arabera), eta eginkizun hauek betez aritzen da lanean Euskal Autonomia Erkidegoan: mehatxu berriak detektatzeko eta garaiz ohartarazteko gaitasuna handituz, informazioaren segurtasuneko gorabeherei erantzunez eta horiek analizatuz, eta euskal gizartearen beharrei erantzuteko prebentzio-neurriak diseinatuz. Helburu horiek lortzeko asmoz, zibersegurtasun-gorabeherak kudeatzera bideratutako hainbat ekimenetan hartzen du parte:

FIRST Improving Security Together
TF-CSIRT Trusted Introducer
CSIRT.es

1. Segurtasun-oharra

Arubak Aruba Orchestrator-erako segurtasun-eguneraketak argitaratu ditu, kalteberatasun ugaritarako zuzenketak egiteko. Hutsegiteek handia eta ertaina bitarteko larritasuna, dute eta mota hauetakoak dira:

- SQL injekzioa
- Pribilegioak eskalatzea
- Cross-site-scripting
- Autentifikazio bypass-a

Kalteberatasun horiek, ustiatuz gero, honako hauetarako erabil daitezke:

- Informazio sentikorra lortzea eta aldatzea
- Erasotzaile bati aukera ematea web-administrazioaren interfazean administrazio-sarbidea lortzeko sistema arriskuan jarriz
- Biktima baten nabigatzailean kode arbitrarioa exekutatzea eragindako interfazearen testuinguruan
- Root gisa komando arbitrarioak exekutatzea sistema osorik arriskuan jarriz
- Erasotzaile bati saioa hasteko aukera ematea erabiltzaile-izen eta pasahitz bat soilik erabiliz eta MFA (faktore anitzeko autentifikazioa) eskakizunak arrakastaz saihestea
- Autentifikatutako erasotzaile bati sisteman egoten uztea uneko saioaren baimenekin

Hauek dira guztien identifikatzaileak: CVE-2022-43519, CVE-2022-43520, CVE-2022-43521, CVE-2022-43522, CVE-2022-43523, CVE-2022-44535, CVE-2022-43524, CVE-2022-44534, CVE-2022-43525, CVE-2022-43526, CVE-2022-43527, CVE-2022-43528, CVE-2022-43529.

2. Eragindako baliabideak

- Aruba EdgeConnect Enterprise Orchestrator (lokala)
- Aruba EdgeConnect Enterprise Orchestrator zerbitzu gisa
- Aruba EdgeConnect Enterprise Orchestrator-SP eta Aruba EdgeConnect Enterprise Orchestrator Global Enterprise Tenant Orchestrators
- Orchestrator 9.2.1.40179 eta lehenagokoa
- Orchestrator 9.1.4.40436 eta lehenagokoa
- Orchestrator 9.0.7.40110 eta lehenagokoa
- Orchestrator 8.10.23.40015 eta lehenagokoa
- Berariaz aipatu ez den Orchestrator-en lehenagoko edozein bertsio.

3. Analisi teknikoa

Hona hemen tratatutako kalteberatasunen xehetasunak:

CVE-2022-43519, CVE-2022-43520, CVE-2022-43521, CVE-2022-43522 eta CVE-2022-43523 kalteberatasunak EdgeConnect Enterprise Orchestrator Interfaz-en webean oinarritutako Aruba-ren Administrazioan autentifikatutako SQL injekzioaren hutsegiteak dira.

Horien guztien metrika hau da:

CVSS Base: 8.8, handia

CWE 89: SQL komando batean erabilitako elementu berezien neutralizazio okerra (SQL injekzioa)

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

- **Eraso-bektorea: Sarea**
- **Erasoaren konplexutasuna: Txikia**
- **Eskatutako pribilegioak:** Txikiak
- **Erabiltzailearekiko interakzioa**: **Bat ere ez**
- **Irismena:** Aldaketarik gabe
- **Konfidentzialtasuna: Handia**
- **Osotasuna: Handia**
- **Erabilgarritasuna: Handia**

CVE-2022-44535: pribilegioen eskalada-kalteberatasuna Enterprise Orchestrator-en webean oinarritutako Aruba EdgeConnect-en kudeaketa-interfazean, eta horrek sistema erabat arriskuan jartzea eragiten du

Kalteberatasunaren metrika hau da:

CVSS Base: 8.8, handia

CWE 284: Sarbide-kontrol desegokia

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

- **Eraso-bektorea: Sarea**
- **Erasoaren konplexutasuna: Txikia**
- **Eskatutako pribilegioak:** Txikiak
- **Erabiltzailearekiko interakzioa**: **Bat ere ez**
- **Irismena:** Aldaketarik gabe
- **Konfidentzialtasuna: Handia**
- **Osotasuna: Handia**
- **Erabilgarritasuna: Handia**

CVE-2022-43524: Aruba EdgeConnect Enterprise Orchestrator-en webean oinarritutako administrazio-interfazearen kalteberatasunak aukera eman lezake autentifikatutako urruneko erasotzaile batek cross-site-scripting (XSS) bat

egiteko interfazearen administrazio-erabiltzaile baten aurka. Exploit arrakastatsu batek aukera ematen dio erasotzaile bati biktima baten nabigatzailean kode arbitrarioa exekutatzeko eragindako interfazearen testuinguruan.

Kalteberatasunaren metrika hau da:

CVSS Base: 8.7, handia

CWE 79: Sarreraren neutralizazio okerra web-orria sortzen den bitartean (Cross-site Scripting)

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

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

CVE-2022-44534: Enterprise Orchestrator-en webean oinarritutako Aruba EdgeConnect-en kudeaketa-interfazean autentifikatutako urruneko kodea exekutatzeko kalteberatasuna, sistema erabat arriskuan jartzen duena.

Kalteberatasunaren metrika hau da:

CVSS Base: 7.2, handia

CWE 94: Kodea sortzearen kontrol desegokia (Kodea injektatzea)

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

- **Eraso-bektorea: Sarea**
- **Erasoaren konplexutasuna: Txikia**
- **Eskatutako pribilegioak:** Goi-mailakoak
- **Erabiltzailearekiko interakzioa: Bat ere ez**
- **Irismena:** Aldaketarik gabe
- **Konfidentzialtasuna: Handia**
- **Osotasuna: Handia**
- **Erabilgarritasuna: Handia**

CVE-2022-43525, CVE-2022-43526 eta CVE-2022-43527 kalteberatasunak Cross Site Site Scripting (XSS) hutsegiteak dira, Aruba EdgeConnect Enterprise Orchestrator-en web-administrazioko interfazekoak.

Kalteberatasunen metrika hau da:

CVSS Base: 6.1, ertaina

CWE 94: Kodea sortzearen kontrol desegokia (Kodea injektatzea)

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

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

CVE-2022-43528: Aruba EdgeConnect Enterprise Orchestrator-en faktore anitzeko autentifikazioa saltatzeko kalteberatasuna.

Kalteberatasunaren metrika hau da:

CVSS Base: 4.8, ertaina

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

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

CVE-2022-43529: Aruba EdgeConnect Enterprise Orchestrator Web-Based Management Interface-n erabiltzaile-saioa behar bezala baliogabetzean errore bat sortzen duen kalteberatasuna.

Kalteberatasunaren metrika hau da:

CVSS Base: 4.6, ertaina

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

- **Eraso-bektorea: Sarea**
- **Erasoaren konplexutasuna: Txikia**
- **Eskatutako pribilegioak:** Txikiak
- **Erabiltzailearekiko interakzioa**: Beharrezkoa
- **Irismena:** Aldaketarik gabe
- **Konfidentzialtasuna:** Txikia
- **Osotasuna:** Txikia
- **Erabilgarritasuna:** Bat ere ez

4. Arintzea / Konponbidea

Kalteberatasunak arintzeko, BCSCk gomendatzen du sistema eta aplikazioak erabilgarri dagoen azken bertsiora eguneratuta edukitzea beti, dagozkion eguneraketak argitaratu bezain laster.

Arubatik, bere segurtasun-oharraren arabera, Aruba EdgeConnect Enterprise Orchestrator bertsio zuzendu hauetako batera eguneratzeko gomendatzen da adierazitako arazo guztiak konpontzeko:

Aruba EdgeConnect Enterprise Orchestrator (lokala)

- Orchestrator 9.2.2.40291 eta ondorengo bertsioak
- Orchestrator 9.1.5.40037 eta ondorengo bertsioak
- Aruba EdgeConnect Enterprise Orchestrator-as-a-Service
- TACek automatikoki sortuko du Arubarako (Silver Peak) euskarri-kasu bat ostatatutako Orchestrator-entzat, eta eguneratu egingo dira.
- Aruba EdgeConnect Enterprise Orchestrator-SP eta ArubaEdgeConnect Enterprise Orchestrator Global Enterprise Tenant Orchestrators

Halaber, azpimarratzen da zerbitzu-hornitzaileek lehen aipatutako bertsio batera eguneratu behar dutela.

5. Erreferentzia gehigarriak

- Aruba-ren segurtasun-oharra
- CVE-2022-43519, CVE-2022-43520, CVE-2022-43521, CVE-2022-43522, CVE-2022-43523, CVE-2022-44535, CVE-2022-43524, CVE-2022-44534, CVE-2022-43525, CVE-2022-43526, CVE-2022-43527, CVE-2022-43528, CVE-2022-43529
- Aruba Orchestrator
- CWE 94
- CWE 79
- CWE 284
- CWE 89


Basque
CyberSecurity
Centre


EUSKO JAURLARITZA
GOBIERNO VASCO


GRUPO
spri
TALDEA