Basque CyberSecurity Centre

Ahultasunak ArubaOS eta Aruba InstantOSen

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

Arubak, empresa inguruneetarako hainbat segurtasun soluziorekin lotutako konpainiak, guztira 13 ahultasun biltzen dituen Segurtasun ohar bat argitaratu du. Horien artean, 8 nabarmendu behar dira, fabrikatzaileak kritikotzat jo baititu. Gainera, guztira 4 akats izan ditu, eta horiei zorroztasun handia eman zaie.

Ahultasunen larritasuna kritikotzat jo da, eta honako identifikatzaile hauetan erregistratu dira:

- CVE-2023-22779, CVE-2023-22780, CVE-2023-22781, CVE-2023-22782, CVE-2023-22783, CVE-2023-22784, CVE-2023-22785 eta CVE-2023-22786: PAPI protocol-ren bidez sartzen diren zerbitzuetan bufer-gainezkatzea eragin dezaketen ahultasunak.

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

- CVE-2023-22787: Ahultasun hori gerta daiteke Aruba InstantOSen zerbitzua ukatzea (DoS) edo PAPI protocol-ren bidez eskuratutako ArubaOSen zerbitzuak ukatzea.
- CVE-2023-22788, CVE-2023-22789 eta CVE-2023-22790: Aruba Instant OSen edo ArubaOS 10en komando-lerroko interfazean kode arbitrarioaren urruneko exekuzioa eragin dezaketen urruntasunak.

Fabrikatzaileak dagoeneko argitaratu ditu dagozkion eguneratzeak, eta, horrela, akats nabarmenak zuzendu ditu. Hori dela eta, kalteberatasun horiek eta beste batzuk prebenitzeko, sistema eta aplikazioak eskuragarri dagoen azken bertsioan eguneratuta izatea gomendatzen da, dagozkien adabakiak argitaratu bezain laster.

2. Azterketa teknikoa

Arubak emandako kalteberatasun kritikoei dagokienez, CVE-2023-22779, CVE-2023-22780, CVE-2023-22781, CVE-2023-22782, CVE-2023-22783, CVE-2023-22784, CVE-2023-22785 eta CVE-2023-22786 erregistratutako akatsak identifikatu dira. Akats horiek Erik de Jong ikertzaileak jakinarazi ditu, PAPI protocolen izandako boundary akats baten ondorioz. Autentifikatu gabeko urruneko erasotzaile batek bereziki diseinatutako paketeak bidal ditzake 8211/UDP portura, bufer-gainezkatzea eragin dezake eta helmugako sisteman administratzaile pribilegioak dituen kode arbitrarioa exekutatu dezake.

Lehen deskribatutako ahultasunak 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: Alta.**
- **Erabilgarritasuna: Alta**

Era berean, lehen ahultasuna, zeinaren larritasuna puntuazio altuarekin kalifikatu baita, CVE-2023-22787an erregistratu da. Daniel Jensen ikertzaileak emandako akatsak, Aruba InstantOS eta ArubaOS 10ek emandako baliabideei zerbitzua ukatzeko erasoa (DoS) ahalbidetu dezake, eta PAPI protocol-ren bidez eskura daitezke. Urruneko erasotzaile batek sarbide-puntu konprometituaren funtzionamendua eten dezake.

CVE-2023-22787 ahultasuna ebaluatzeko metrikak honela osatuta daude:

CVSS Oinarria: 7.5

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

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

Azkenik, CVE-2023-22788, CVE-2023-22789 eta CVE-2023-22790 sektoreetan identifikatutako ahultasunak ere kritikotasun handiarekin kalifikatu ditu fabrikatzaileak. Akats horiek, Daniel Jensenek jakinarazitakoak, ArubaOS eta Aruba InstantOSen komandoen lineako interfazean sarrera desegokia baliozkotzeak eragiten ditu. Urruneko erasotzaile batek eragindako interfazearen bidez bereziki diseinatutako argudioak pasa ditzake, eta helmugako sisteman administratzaile pribilegioak dituzten komando arbitrarioak exekutatu.

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

Azkenik, honako hauek dira aurreko ahultasunek eragindako produktuak:

- ArubaOS 10.3.10 bertsioa eta aurrekoak.
- Aruba InstantOS 8.10.0.4 bertsioa eta aurrekoak, bertsio guztiak 8.9.X, 8.8.X, 8.7.X, 8.6.0.19 eta aurrekoak, bertsio guztiak 8.5.X eta 8.4.X, 6.5.4.23 eta aurrekoak eta 6.4.4.8-4.2.4.20 eta aurrekoak.

3. Arintzea / Mitigazioa

Ohikoa denez, ahultasun horiek eta beste batzuk prebenitzeko, sistemak eta aplikazioak eskuragarri dagoen azken bertsioan eguneratuta izatea gomendatzen da, dagozkion eguneratzeak argitaratu bezain laster.

Horretarako, ArubaOS bertsio nabarmen hauetan eguneratu beharko da:

- ArubaOS 10.4.X: 10.4.0.0 bertsioa edo berriagoa eguneratu.
- Aruba InstantOS 8.11.X: 8.11.0.0 bertsioa edo berriagoa eguneratu.
- Aruba InstantOS 8.10.X: 8.10.0.3 bertsioa edo berriagoa eguneratu.

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

CVE-2023-22779, CVE-2023-22780, CVE-2023-22781, CVE-2023-22782, CVE-2023-22783, CVE-2023-22784, CVE-2023-22785 eta CVE-2023-22786 ahultasunei dagokienez, erabiltzaileek *cluster security* funtzioa gaitu beharko dute 8.X edo 6.X bertsioa duten Aruba InstantOS gailuetan *cluster-security* komandoaren bidez. ArubaOS 10 gailuetarako, konexio ez-fidagarri horien UDP/8211 porturako sarbidea blokeatu behar da.

Altua moduan katalogatutako CVE-2023-22787ahultasunari dagokionez, administratzaileek UDP/8211 atakarako sarbidea blokeatu beharko dute fidagarriak ez diren konexioetarako.

Horrez gain, fabrikatzaileak gomendatzen du web-ean oinarritutako CLI kudeaketa interfazeak 2. mailako segmentu/VLAN batera mugatzea, eta 3. mailako edo hortik gorako suebaki politiken bidez kontrolatzea.

Azkenik, Segurtasun soluzio alternatibo aipagarriak aplikatzen dituzten erabiltzaileentzat, bertsio hauek aplikatu beharko dituzte, *PAPI Protocol-en* buferra gainezka egiteko ahultasunetarako izan ezik.

- ArubaOS 10.4.X: 10.4.0.0 bertsioa edo berriagoa eguneratu.
- ArubaOS 10.3.X: 10.3.1.1 bertsioa edo berriagoa eguneratu.
- Aruba InstantOS 8.11.X: 8.10.0.5 bertsioa edo berriagoa eguneratu.
- Aruba InstantOS 8.6.X: 8.6.0.20 bertsioa edo berriagoa eguneratu.
- Aruba InstantOS 6.5.X: 6.5.4.24 bertsioa edo berriagoa eguneratu.
- Aruba InstantOS 6.4.X: 6.4.4.8-4.2.4.21 bertsioa edo berriagoa eguneratu.

4. Erreferentzia osagarriak

- ARUBA-PSA-2023-006.
- ArubaOS.
- PAPI Protocol.
- Zer da zerbitzua ukatzeko erasoa (DoS)?
- Boundary error.
- 8211/UDP ataka.
- CWE-121: Stack-based Buffer Overflow.
- CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection').
- CWE-20: Improper Input Validation.
- Cluster-security.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA