cyber zaintza
BASQUE CYBERSECURITY AGENCY

Kalteberatasunak ArubaOS-en

CYBERZAINTZA-ABISUAK

TLP: CLEAR

www.zibersegurtasun.eus

EUSKO JAURLARITZA
GOBIERNO VASCO

EDUKI-TAULA

Erantzukizunetik salbuesteko klausula

Dokumentu hau Zibersegurtasunaren Euskal Agentziak erakundeen eta herritar interesatuen segurtasunaren alde beharrezkotzat jotzen dituen alertak gizarteratzeko helburuz sortu da. Zibersegurtasunaren Euskal Agentzia ezin da jo, inola ere, Zibersegurtasunerako Euskal Agentziaren webgunean emandako informazioaren edo erreferentzia egiten zaien teknologien erabilerak eragin ditzaketen kalteen erantzuletzat, ezta kanpoko web-orrialdeetarako esteka bidez sartutako bestelako informazioaren, software produktuen edo Zibersegurtasunaren Euskal Agentziaren webgunean edo alertan ager daitezkeen beste edozein informazioaren erantzuletzat ere. Edonola ere, alertaren edukiak eta mezu elektronikoen bidez eman litezkeen erantzunak iritzi eta gomendioak dira, hemen bildutako terminoekin bat etorrita, eta emandako informazioaren ondorioz ezingo da eragin juridiko loteslerik sortu.

Salmenta debekatzeko klausula

Guztiz debekatuta dago saltzea edo edozein etekin ekonomiko lortzea, baina horrek ez du eragotziko dokumentu hau kopiatzeko, banatzeko, zabaltzeko edo gizarteratzeko aukera.

1. Laburpen exekutiboa

Aruba networkek segurtasun-abisu bat argitaratu du **ArubaOS** (Aruba Networksek garatutako sistema eragilea) produktuei eta **SD-WAN** softwareari (SD-WAN softwareak definitutako tokiko sarea) eragiten dieten **kalteberatasun ugariak** zuzentzeko.

Garrantzitsuenen artean, **larritasun handiko 4 kalteberatasun** daude: CVE-2024-1356, CVE-2024-25611, CVE-2024-25612 eta CVE-2024-25613. Kalteberatasun horiek azpian dagoen hostean komando arbitrarioak exekutatzeko aukera eman diezaiekete urruneko erabiltzaile kautotuei, root gisa; hala, arriskuan jar dezakete sistema osoa. Ondorioz, kalteberatasun guztiak mehatxu oso larriak dira kalteberatasun horien ustiapenak kaltetu ditzakeen sistemetako konfidentzialtasunerako, segurtasunerako eta eskuragarritasunerako.

Fabrikatzaileak dagoeneko argitaratu ditu dagozkion eguneratzeak eta arintze-neurriak, eta, horrela, akats nabarmenak zuzendu ditu. Beraz, kalteberatasun horiek eta beste batzuk prebenitzeko, sistema eta aplikazioak eskuragarri dagoen azken bertsioaren arabera eguneratuta izatea gomendatzen da, dagozkien adababiak argitaratu bezain laster.

2. Kaltetutako baliabideak

ArubaOSen bertsio hauei eragiten diete azaldutako kalteberatasunek:

- ArubaOS 10.5.x.x: 10.5.0.1 eta aurrekoak
- ArubaOS 10.4.x.x: 10.4.0.3 eta aurrekoak
- ArubaOS 8.11.x.x: 8.11.2.0 eta aurrekoak
- ArubaOS 8.10.x.x: 8.10.0.9 eta aurrekoak

Halaber, nabarmentzekoa da ArubaOSen eta SD-WANen bertsio batzuen mantentze-aldia amaitu egin dela. Hortaz, kalteberatasun hauek eragiten badiete ere, eguneratze honek ez ditu zuzentzen. Honakoak dira:

- ArubaOS 10.3.x.x: bertsio guztiak.
- ArubaOS 8.9.x.x: bertsio guztiak.
- ArubaOS 8.8.x.x: bertsio guztiak.
- ArubaOS 8.7.x.x: bertsio guztiak.
- ArubaOS 8.6.x.x: bertsio guztiak.
- ArubaOS 6.5.4.x: bertsio guztiak.
- SD-WAN 8.7.0.0-2.3.0.x: bertsio guztiak.
- SD-WAN 8.6.0.4-2.2.x.x: bertsio guztiak.

Kalteberatasun horiek ez diete eragiten HPE Aruba Networkingenak diren baina aurreko zerrendan berariaz aipatuta ez dauden produktuei.

3. Azterketa teknikoa

Abisu honetan landutako kalteberatasun garrantzitsuenen xehetasunak hauek dira:

CVE-2024-1356, CVE-2024-25611, CVE-2024-25612, CVE-2024-25613: kautotutako komandoak txertatzearekin lotutako kalteberatasunak, ArubaOSen komandoen lerroaren interfazeari eragiten diotenak. Kalteberatasun horiek ustiatuz gero, azpian dagoen sistema eragilean erabiltzaile pribilegiatu gisa komando arbitrarioak exekutatzea ahalbidetu liteke.

Kalteberatasunaren azterketaren neurketak honako hauek ditu:

Oinarrizko CVSSa: **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**
- **Beharrezko pribilegioak:** Altuak
- **Interakzioa erabiltzailearekin: Bat ere ez**
- **Aplikazio-eremua:** Aldaketarik gabe
- **Konfidentzialtasuna Altua**
- **Integritatea: Altua**
- **Eskuragarritasuna: Altua**

4. Arintzea / Konponbidea

Ohikoa den bezala, kalteberatasun horiek eta beste batzuk prebenitzeko, sistemak eta aplikazioak beti eskuragarri dagoen azken bertsiora eguneratuta izatea gomendatzen da, dagozkien eguneratzeak argitaratu bezain laster.

Mugikortasun Kontroladoreak, Mugikortasun Eroaleak eta Pasabideak ArubaOSen honako bertsioren batera eguneratzea gomendatzen du HPE Arubak:

- ArubaOS 10.5.x.x: 10.5.1.0 eta hurrengoak.
- ArubaOS 10.4.x.x: 10.4.1.0 eta hurrengoak.
- ArubaOS 8.11.x.x: 8.11.2.1 eta hurrengoak.
- ArubaOS 8.10.x.x: 8.10.0.10 eta hurrengoak.

5. Erreferentzia gehigarriak

- Segurtasun-abisua.
- CVE-2024-1356.
- CVE-2024-25611.
- CVE-2024-25612.
- CVE-2024-25613.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY