Kalteberatasunak Arubaren ClearPass Policy Managerren

CYBERZAINTZA-ABISUAK

TLP: CLEAR

www.zibersegurtasun.eus

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

1. Laburpen exekutiboa

Aruba networkek segurtasun-abisu bat argitaratu du Clearpass Policy Manager produktuari eragiten dioten **kalteberatasun ugariak** zuzentzeko. Sarbide-politiken plataforma da **Clearpass Policy Manager**, eta sareko kontrola eskaintzen du, roletan eta gailuetan oinarrituta.

Garrantzitsuenen artean, **larritasun kritikoko 1 kalteberatasun (**CVE-2023-50164**)** eta **larritasun handiko 5 kalteberatasun** daude (CVE-2024-26294, CVE-2024-26295, CVE-2024-26296, CVE-2024-26297, CVE-2024-26298). 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 adabakiak argitaratu bezain laster.

2. Kaltetutako baliabideak

Clearpass Policy Managerrek exekutatutako eta kalteberatasun hauek kaltetutako **software bertsio** hauek **bizi-zikloaren amaierara heldu dira,** eta HPE Arubak ez die adabakirik aplikatuko:

- ClearPass Policy Manager 6.12.x: 6.12.0
- ClearPass Policy Manager 6.11.x: 6.11.6 eta aurrekoak.
- ClearPass Policy Manager 6.10.x: ClearPass 6.10.8 Hotfix Q4 2023 (segurtasun-arazoetarako) eta aurrekoak
- ClearPass Policy Manager 6.9.x: ClearPass 6.9.13 Hotfix Q4 2023 (segurtasun-arazoetarako) eta aurrekoak

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-2023-50164: komandoak txertatzean datzan kalteberatasuna. Erasotzaileak artxiboak kargatzeko parametroak manipulatu ditzake, bideen trabesia ahalbidetzeko. Eta, kasu batzuetan, urruneko kode bat exekutatzeko erabil daitekeen fitxategi gaizto bat kargatzea eragin dezake horrek. Ez da baieztatu kalteberatasun honek ClearPass Policy Managerren duen inpaktua, baina Apache Strutsen bertsioa eguneratu egin da, inpaktua arintzeko. HPE Aruba Networkingek ez du izan kalteberatasun honen inolako ustiapen gaiztoren berririk.

Kalteberatasunaren azterketaren neurketak honako hauek ditu:

CWE 552: Files or Directories Accessible to External Parties

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

CVE-2024-26294, CVE-2024-26295, CVE-2024-26296, CVE-2024-26297, CVE-2024-26298: Cross-Site Scriptingen (XSS) kalteberatasun multzoa, ClearPass Policy Managerren webgunea kudeatzeko interfazean. Azpian dagoen hostean komando arbitrarioak exekutatzeko aukera ematen die urruneko erabiltzaile kautotuei. Kalteberatasuna arrakastaz ustiatuz gero, erasotzaileak komando arbitrarioak exekutatu litzake azpian dagoen sistema eragilean, root gisa. Horrek arriskuan jarriko luke sistema osoa.

Kalteberatasunaren azterketaren neurketak honako hauek ditu:

CWE 552: Files or Directories Accessible to External Parties

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.

ClearPass Policy plataforma honako bertsioren batera eguneratzeko gomendatzen du HPE Arubak:

- ClearPass Policy Manager 6.12.x: 6.12.1 eta hurrengoak.
- ClearPass Policy Manager 6.11.x: 6.11.7 eta hurrengoak.
- ClearPass Policy Manager 6.10.x: 6.10.8 Hotfix Parche 8 Q1 2024 (segurtasun-arazoetarako) eta hurrengoak.
- ClearPass Policy Manager 6.9.x: 6.9.13 Hotfix Parche 7 T1 2024 (segurtasun-arazoetarako) eta hurrengoak.

5. Erreferentzia gehigarriak

- Segurtasun-abisua.
- CVE-2023-50164.
- CVE-2024-26294.
- CVE-2024-26295.
- CVE-2024-26296.
- CVE-2024-26297.
- CVE-2024-26298.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY