مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in HPE Aruba Networking ArubaOS
Tracking #:432315686
Date:08-03-2024

TLP: WHITE

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Multiple Vulnerabilities in HPE Aruba Networking ArubaOS that could be exploited to gain unauthorized access to vulnerable systems.

TECHNICAL DETAILS:

Vulnerabilities Details:
1.CVE-2024-1356, CVE-2024-25611, CVE-2024-25612, CVE-2024-25613
- CVSSv3 Score: 7.2 High
- Authenticated command injection vulnerabilities in the ArubaOS CLI could allow attackers to execute arbitrary commands with elevated privileges.

2.CVE-2024-25614
- CVSSv3 Score: 5.5 Medium
- An arbitrary file deletion vulnerability in the ArubaOS CLI could allow attackers to delete files on the system, potentially leading to denial-of-service (DoS).

3.CVE-2024-25615
- CVSSv3 Score: 5.3 Medium
- An unauthenticated DoS vulnerability in the ArubaOS Spectrum service (accessed via PAPI) could allow attackers to disrupt normal operation of the service.

4CVE-2024-25616
- CVSSv3 Score: 3.7 Low
- A vulnerability in certain ArubaOS configurations could lead to partial disclosure of sensitive information during IKE_AUTH negotiation.

Affected Versions:
- ArubaOS 10.5.x.x: 10.5.0.1 and below
- ArubaOS 10.4.x.x: 10.4.0.3 and below
- ArubaOS 8.11.x.x: 8.11.2.0 and below
- ArubaOS 8.10.x.x: 8.10.0.9 and below

Fixed Versions:
- ArubaOS 10.5.x.x: 10.5.1.0 and above
- ArubaOS 10.4.x.x: 10.4.1.0 and above
- ArubaOS 8.11.x.x: 8.11.2.1 and above
- ArubaOS 8.10.x.x: 8.10.0.10 and above

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by HPE Aruba Networking.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2024-002.txt