مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates- Critical Vulnerabilities HPE Aruba Networking ArubaOS

Tracking #:432315807

Date:02-05-2024

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 affected systems.

TECHNICAL DETAILS:

HPE Aruba Networking has identified and addressed multiple vulnerabilities affecting Aruba Mobility Conductor (formerly Mobility Master), Mobility Controllers, WLAN Gateways, and SD-WAN Gateways. These vulnerabilities can be exploited by a remote attacker to execute arbitrary code or cause denial-of-service (DoS) conditions.

Vulnerabilities Details:

- **Unauthenticated Buffer Overflow Vulnerabilities (Critical, CVSSv3: 9.8):**
  - CVE-2024-26305: Utility Daemon (PAPI Protocol)
  - CVE-2024-26304: L2/L3 Management Service (PAPI Protocol)
  - CVE-2024-33511: Automatic Reporting Service (PAPI Protocol)
  - CVE-2024-33512: Local User Authentication Database (PAPI Protocol)
  - These vulnerabilities allow remote attackers to execute arbitrary code with privileged access on the underlying operating system.
- **Unauthenticated Denial-of-Service (DoS) Vulnerabilities (Medium, CVSSv3: 5.3 - 5.9):**
  - CVE-2024-33513, CVE-2024-33514, CVE-2024-33515: AP Management Service (PAPI Protocol)
  - CVE-2024-33516: Auth Service (PAPI Protocol)
  - CVE-2024-33517: Radio Frequency Manager Service (PAPI Protocol)
  - CVE-2024-33518: Radio Frequency Daemon (PAPI Protocol)
  - These vulnerabilities allow remote attackers to disrupt normal operation of affected services.

Affected Versions:

- ArubaOS 10.5.x.x: 10.5.1.0 and below
- ArubaOS 10.4.x.x: 10.4.1.0 and below
- ArubaOS 8.11.x.x: 8.11.2.1 and below
- ArubaOS 8.10.x.x: 8.10.0.10 and below

End-of-Maintenance (EOL) Software Versions (Not Patched):

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

Fixed Versions:

- ArubaOS 10.6.x.x: 10.6.0.0 and above
- ArubaOS 10.5.x.x: 10.5.1.1 and above

- ArubaOS 10.4.x.x: 10.4.1.1 and above
- ArubaOS 8.11.x.x: 8.11.2.2 and above
- ArubaOS 8.10.x.x: 8.10.0.11 and above

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released 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-2024-004.txt