مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in HPE Aruba Networking Access Points

Tracking #:432316171

Date:21-08-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed critical vulnerabilities in HPE Aruba Networking Access Points that could be exploited to remotely execute code or cause a denial-of-service condition on affected devices.

TECHNICAL DETAILS:

Vulnerabilities Details:

- **CVE-2024-42393, CVE-2024-42394-**Unauthenticated Stack-Based Buffer Overflow Remote Command Execution (RCE) in the Soft AP Daemon Service Accessed by the PAPI Protocol.
  - CVSS Score **9.8 Critical**
  - A stack-based buffer overflow vulnerability exists in the Soft AP Daemon Service, which can be exploited by an unauthenticated attacker to execute arbitrary commands. Successful exploitation could lead to complete system compromise.

- **CVE-2024-42395-**Unauthenticated Stack-Based Buffer Overflow Remote Command Execution (RCE) in the AP Certificate Management Service Accessed by the PAPI Protocol.
  - CVSS Score **9.8 Critical**
  - A stack-based buffer overflow vulnerability exists in the AP Certificate Management Service, allowing an unauthenticated attacker to execute arbitrary commands. Successful exploitation could result in complete system compromise.

Affected Products:

- HPE Aruba Networking - Aruba Access Points running InstantOS and ArubaOS 10

Affected Versions:

- ArubaOS 10.6.x.x: 10.6.0.0 and below
- ArubaOS 10.4.x.x: 10.4.1.3 and below
- InstantOS 8.12.x.x: 8.12.0.1 and below
- InstantOS 8.10.x.x: 8.10.0.12 and below
- End-of-Maintenance (EoM) Products:
  - ArubaOS 10.5.x.x: all
  - ArubaOS 10.3.x.x: all
  - InstantOS 8.11.x.x: all
  - InstantOS 8.9.x.x: all
  - InstantOS 8.8.x.x: all
  - InstantOS 8.7.x.x: all
  - InstantOS 8.6.x.x: all
  - InstantOS 8.5.x.x: all
  - InstantOS 8.4.x.x: all
  - InstantOS 6.5.x.x: all
  - InstantOS 6.4.x.x: all

Fixed Versions:

- ArubaOS 10.6.x.x: 10.6.0.1 and above
- ArubaOS 10.4.x.x: 10.4.1.4 and above
- InstantOS 8.12.x.x: 8.12.0.2 and above
- InstantOS 8.10.x.x: 8.10.0.13 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://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04678en_us&docLocale=en_US