مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in HPE Aruba Networking Access Points

Tracking #:432316483
Date:07-11-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in HPE Aruba Networking Access Points that could be exploited to gain unauthorized access, execute malicious code, and potentially take full control of affected devices.

TECHNICAL DETAILS:

Vulnerabilities Details:

1. Unauthenticated Command Injection in CLI Service (CVE-2024-42509)
    - **Severity**: Critical
    - **CVSS v3.x Score**: 9.8
    - **Description**: This vulnerability allows unauthenticated remote attackers to execute arbitrary commands via the CLI service accessed through the PAPI protocol.
    - **Impact**: An attacker can potentially gain full control over the affected device without authentication.
2. Unauthenticated Command Injection via PAPI Protocol (CVE-2024-47460)
    - **Severity**: Critical
    - **CVSS v3.x Score**: 9.0
    - **Description**: Similar to CVE-2024-42509, this vulnerability enables unauthenticated command injection through the PAPI protocol.
    - **Impact**: Attackers can execute arbitrary commands on the device without authentication, potentially leading to complete system compromise.
3. Authenticated Remote Command Execution (CVE-2024-47461)
    - **Severity**: High
    - **CVSS v3.x Score**: 7.2
    - **Description**: An authenticated command injection vulnerability exists in the Instant AOS-8 and AOS-10 command line interface
    - **Impact**: A successful exploitation allows execution of arbitrary commands as a privileged user on the underlying operating system, potentially leading to full system compromise
4. Arbitrary File Creation Leading to RCE (CVE-2024-47462, CVE-2024-47463)
    - **Severity**: High
    - **CVSS v3.x Score**: 7.2
    - **Description**: These vulnerabilities allow authenticated attackers to create arbitrary files, potentially leading to remote command execution.
    - **Impact**: Attackers can potentially escalate privileges and execute malicious code on the affected systems.
5. Authenticated Path Traversal (CVE-2024-47464)
    - **Severity**: Medium
    - **CVSS v3.x Score**: 6.8
    - **Description**: This vulnerability enables authenticated attackers to gain unauthorized access to files through path traversal.
    - **Impact**: Attackers can potentially access sensitive files and information outside the intended directory structure.

Affected Products:

HPE Aruba Networking - Access Points running Instant AOS-8 and AOS-10
Affected Software Version(s):

- AOS-10.4.x.x: 10.4.1.4 and below

- Instant AOS-8.12.x.x: 8.12.0.2 and below
- Instant AOS-8.10.x.x: 8.10.0.13 and below

The following end-of-maintenance (EoM) versions are affected by these vulnerabilities and will not receive updates:

- AOS-10.6.x.x: all
- AOS-10.5.x.x: all
- AOS-10.3.x.x: all
- Instant AOS-8.11.x.x: all
- Instant AOS-8.9.x.x: all
- Instant AOS-8.8.x.x: all
- Instant AOS-8.7.x.x: all
- Instant AOS-8.6.x.x: all
- Instant AOS-8.5.x.x: all
- Instant AOS-8.4.x.x: all
- Instant AOS-6.5.x.x: all
- Instant AOS-6.4.x.x: all

Fixed Versions:

- AOS-10.7.x.x: 10.7.0.0 and above
- AOS-10.4.x.x: 10.4.1.5 and above
- Instant AOS-8.12.x.x: 8.12.0.3 and above
- Instant AOS-8.10.x.x: 8.10.0.14 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://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04722en_us&docLocale=en_US