مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - HPE Aruba Networking

Tracking #:432316624

Date:12-12-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that HPE Aruba Networking has released security updates to patch multiple vulnerabilities in AirWave Management Platform.

TECHNICAL DETAILS:

HPE Aruba Networking has released a software update to address multiple security vulnerabilities affecting the HPE Aruba Networking AirWave Management Platform. These vulnerabilities, if exploited, could potentially allow unauthorized access and compromise the security of network infrastructure.

Vulnerabilities Details:
CVE-2024-54008: Authenticated Remote Code Execution (RCE)
Severity: High
CVSS Score: 7.2
An authenticated Remote Code Execution vulnerability exists in the AirWave CLI. Successful exploitation could allow a remote authenticated threat actor to execute arbitrary commands as a privileged user on the underlying host

CVE-2022-25844: Regular Expression Denial of Service (ReDoS)
Severity: Medium
CVSS Score: 5.3
The Angular package (versions after 1.7.0) is vulnerable to a Regular Expression Denial of Service (ReDoS) attack. This can occur by providing a custom locale rule that allows the assignment of an extremely high value to the posPre parameter in NUMBER_FORMATS.PATTERNS posPre.

Affected Versions:
HPE Aruba Networking AirWave Management Platform

- 8.3.0.3 and below

Fixed Versions:
HPE Aruba Networking AirWave Management Platform

- 8.3.0.4 and above

Workaround

- Restricting the CLI and web-based management interfaces to a dedicated layer 2 segment/VLAN.
- Controlling access through firewall policies at layer 3 and above

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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=hpesbnw04765en_us&docLocale=en_US