مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - HPE Aruba Products

Tracking #:432316749

Date:16-01-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed two high-severity vulnerabilities have been discovered in HPE Aruba Networking AOS Controllers and Gateways that could allow authenticated attackers to execute arbitrary code or commands on affected systems.

TECHNICAL DETAILS:

Hewlett Packard Enterprise (HPE) has issued a security advisory concerning multiple vulnerabilities affecting ArubaOS (AOS) controllers and gateways used in HPE Aruba Networking products.

Key Details

- **CVE-2025-23051**: Authenticated parameter injection vulnerability in the web-based management interface
- **CVE-2025-23052**: Authenticated command injection vulnerability in the command line interface
- Both vulnerabilities have a CVSS v3.1 base score of 7.2 (High)
- Affected products include Mobility Conductors, Mobility Controllers, and WLAN and SD-WAN Gateways managed by HPE Aruba Networking Central

Fixed Versions:

- AOS-10.7.x.x: 10.7.0.0 and above
- AOS-10.4.x.x: 10.4.1.5 and above
- AOS-8.12.x.x: 8.12.0.3 and above
- AOS-8.10.x.x: 8.10.0.15 and above

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by HPE.

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=hpesbnw04723en_us&docLocale=en_US