مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Command Injection Vulnerabilities in HPE Aruba

Tracking #:432316719

Date:09-01-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed HPE Aruba Networking has published a security advisory addressing command injection vulnerabilities in the 501 Wireless Client Bridge.

TECHNICAL DETAILS:

HPE Aruba Networking has published a security advisory addressing command injection vulnerabilities in the 501 Wireless Client Bridge. These flaws could allow authenticated attackers to execute arbitrary commands with privileged access on affected devices. A proof-of-concept exploit has been publicly released, increasing the urgency for patching.

Vulnerabilities Overview:

- CVE-2024-54006 & CVE-2024-54007
- Severity: Both vulnerabilities are rated as High (CVSS score 7.2).
- Impact: These vulnerabilities allow authenticated attackers with administrative privileges to execute arbitrary commands on the 501 Wireless Client Bridge. Successful exploitation could provide attackers with full control over the device's underlying operating system.
- Exploitability: Exploitation requires administrative credentials, but the attacker can gain complete control over the device once successfully exploited.

Affected Software Versions:

- 501 Wireless Client Bridge V2.1.1.0-B0030 and below

Resolution:

- V2.x.x.x: V2.1.2.0-B0033 and above

RECOMMENDATIONS:

- Immediately upgrade affected devices to fixed version.
- Conduct a thorough security audit of all Aruba devices in your network.
- Monitor for any suspicious activities or unauthorized access attempts.
- Implement strong authentication mechanisms and regularly rotate administrative credentials.

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=hpesbnw04763en_us&docLocale=en_US