مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in HPE Aruba Networking VIA Client

Tracking #:432317039

Date:04-04-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that HPE Aruba Networking has identified multiple vulnerabilities in the Virtual Intranet Access (VIA) client software for Microsoft Windows, MacOS, Linux, and iOS platforms. These vulnerabilities could allow unauthorized access to files and remote code execution, posing significant risks to affected systems.

TECHNICAL DETAILS:

Vulnerabilities Details:

1. **CVE-2024-3661 ("TunnelVision")**
    - **Severity:** High (CVSS Score: 7.1)
    - Unauthenticated remote code execution via DHCP protocol vulnerabilities. Attackers may intercept, disrupt, or modify VPN traffic.
    - **Affected Systems:** Windows, MacOS, Linux, iOS (Android unaffected).
2. **CVE-2025-25041**
    - **Severity:** Medium (CVSS Score: 5.5)
    - Arbitrary file overwrite as NT AUTHORITY\SYSTEM on Windows clients, potentially leading to denial-of-service conditions.
    - **Affected Systems:** Windows only (Linux and Android unaffected).

Fixed Versions:

- For CVE-2024-3661 (Linux, MacOS, iOS, and Microsoft Windows): Upgrade to HPE Aruba Networking VIA client version 4.7.2 or higher.
- For CVE-2025-25041 (Microsoft Windows only): Upgrade to HPE Aruba Networking VIA client version 4.7.2 or higher.

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=hpesbnw04841en_us&docLocale=en_US