DAP-1620 Firmware Patch Notes

Firmware: v1.06B04 BETA
Hardware: Ax
Date: March 16, 2018

Note:
This release is to patch the WPA2 Key Reinstallation Attack (KRACK) Security Vulnerabilities affecting this product.

The beta firmware will be followed up by a fully quality test release in approximately 4 weeks.

Problems Resolved:

A WPA2 wireless protocol vulnerability was reported to CERT//CC and public disclosed as: **VU#228519** - Wi-Fi Protected Access II (WPA2) handshake traffic can be manipulated to induce nonce and session key reuse.

The following CVE IDs have been assigned to VU#228519. These vulnerabilities in the WPA2 protocol:

- CVE-2017-13077: reinstallation of the pairwise key in the Four-way handshake
- CVE-2017-13078: reinstallation of the group key in the Four-way handshake
- CVE-2017-13079: reinstallation of the integrity group key in the Four-way handshake
- CVE-2017-13080: reinstallation of the group key in the Group Key handshake
- CVE-2017-13081: reinstallation of the integrity group key in the Group Key handshake
- CVE-2017-13082: accepting a retransmitted Fast BSS Transition Re-association Request and reinstalling the pairwise key while processing it
- CVE-2017-13084: reinstallation of the STK key in the PeerKey handshake

- CVE-2017-13086: reinstallation of the Tunneled Direct-Link Setup (TDLS) PeerKey (TPK) key in the TDLS handshake

- CVE-2017-13087: reinstallation of the group key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame

- CVE-2017-13088: reinstallation of the integrity group key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame

---