



DAP-1620 Firmware Patch Notes

Firmware: 1.06B04 BETA

Hardware: Ax

Date: March 16, 2018

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

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

DISCLAIMER: Please note that this is a device beta software, beta firmware, or hot-fix release which is still undergoing final testing before its official release. The beta software, beta firmware, or hot-fix is provided on an “as is” and “as available” basis and the user assumes all risk and liability for use thereof. D-Link does not provide any warranties, whether express or implied, as to the suitability or usability of the beta firmware. D-Link will not be liable for any loss, whether such loss is direct, indirect, special or consequential, suffered by any party as a result of their use of the beta firmware.