DIR-878 Firmware Patch Notes

Firmware: FW1.02B01 BETA
Hardware: Ax
Date: November 29, 2017

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

This patch also included fixes for DNSmasq vulnerability:

- CVE-2017-14491 – Remote code execution in the DNS subsystem that can be exploited from the other side of the internet against public-facing systems and against stuff on the local network. The previously latest version had a two-byte overflow bug, which could be leveraged, and all prior builds had an unlimited overflow.

- CVE-2017-14492 – The second remote code execution flaw works via a heap-based overflow.

- CVE-2017-14493 – Google labels this one as trivial to exploit. It's a stack-based buffer overflow vulnerability that enables remote code execution if it's used in conjunction with the flaw below.

- CVE-2017-14494 – This is an information leak in DHCP which, when using in conjunction with CVE-2017-14493, lets an attacker bypass the security mechanism ASLR and attempt to run code on a target system.

- CVE-2017-14495 – A limited flaw this one, but can be exploited to launch a denial of service attack by exhausting memory. Dnsmasq is only vulnerable, however, if the command line switches --add-mac, --add-cpe-id or --add-subnet are used.

- CVE-2017-14496 – Here the DNS code performs invalid boundary checks, allowing a system to be crashed using an integer underflow leading to a huge memcpy() call. Android systems are affected if the attacker is local or tethered directly to the device.

- CVE-2017-13704 – A large DNS query can crash the software
