DIR-850L Firmware Patch Notes

Firmware: FW1.21B06
Hardware: A1
Date: November 16, 2017

Note:
You must update your router to firmware versions 1.15B04 and 1.20B03 first before updating this firmware. Both are available in the 1.21B06 package.

Problems Resolved:

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.

Enhancements:

None

Known Issues:

When registering to mydlink using the setup wizard, mydlink.com will load and you may get a "page cannot be displayed" error or a certificate error. Simply close the window, reopen your web browser, and go to mydlink.com.