DIR-601 Firmware Release Notes

Firmware: FW v2.02B01 BETA 01

Hardware: Rev.B1

Notes:

Discovered by Richard Rogerson (rogerson at packetlabs dot net) on April 10, 2015

Problems Resolved:

1. Authentication Bypass: Through modifying the post to my_cgi.cgi, it is possible to include as many table_name references as required to retrieve the Admin credentials, wireless ssid, and key where applicable.

2. Captcha Bypass: During login, the captcha challenge and response are posted together to my_cgi.cgi allowing an attacker to hardcode these entries to perform a brute force attack. Please note this assumes the captcha feature has been enabled by user, which is disabled by default.

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.