DIR-868L Firmware Patch Notes

Firmware: v1.20B01 BETA
Hardware: Ax
Date: February 28, 2018

Installation:
This patch requires two firmware updates. First upgrade with the *DIR868LA1_FW113b01_middle.bin* file. Then upgrade with *DIR868LA1_FW120b01.bin*.

Notes:

Reported: 01/14/2018
Discovered by: Kaixiang Zhang of Qihoo 360 Gear Team

Problems Resolved:

CVE-2018-6527
XSS vulnerability in htdocs/webinc/js/adv_parent_ctrl_map.php allowing remote attackers to read a cookie via a crafted deviceid parameter to soap.cgi in the following:

DIR-868L - A1 FW112b04 and previous versions
DIR-865L - REVA_FIRMWARE_PATCH_1.08.B01 and previous versions
DIR-860L - A1 FW110b04 and previous versions

CVE-2018-6528
XSS vulnerability in htdocs/webinc/body/bsc_sms_send.php allowing remote attackers to read a cookie via a crafted receiver parameter to soap.cgi in the following:

DIR-868L - A1 FW112b04 and previous versions
DIR-865L - REVA_FIRMWARE_PATCH_1.08.B01 and previous versions
DIR-860L - A1 FW110b04 and previous versions

CVE-2018-6529
XSS vulnerability in htdocs/webinc/js/bsc_sms_inbox.php allowing remote attackers to read a cookie via a crafted Treturn parameter to soap.cgi in the following:

DIR-868L - FW112b04 and previous versions
DIR-865L - REVA_FIRMWARE_PATCH_1.08.B01and previous versions
DIR-860L - FW110b04 and previous versions

CVE-2018-6530
OS command injection vulnerability in soap.cgi (soapcgi_main incgibin) allowing remote attackers to execute arbitrary OS commands via the service parameter in the following:

DIR-880L - REVA_FIRMWARE_PATCH_1.08B04 and previous versions
DIR-868L - A1 FW112b04 and previous versions
DIR-865L - REVA_FIRMWARE_PATCH_1.08.B01 and previous versions
DIR-860L - A1 FW110b04 and previous versions

Enhancements:
None

Known Issues:
None