pwnninja Update DIR-846_SetMasterWLanSettingsCI.md History

1 contributor

26 lines (16 sloc) | 1.23 KB

Vendor:D-Link https://www.dlink.com

Product:D-Link Router DIR-846

Tested Version:DIR-846 A1_100.26 and maybe other versions

Type:OS Command Injection

Author:heshizhi(Wuhan University)

I found an OS command injection vulnerability in the router's web server--lighttpd. While processing the "ssid0" and "ssid1" parameter for a post request to /HNAP1, the value is passed to function exec(). A remote attacker can post specific data, which will execute arbitrary commands such as "telnetd","reboot","ifconfig". The router will be compromised easily.

The details are shown below:

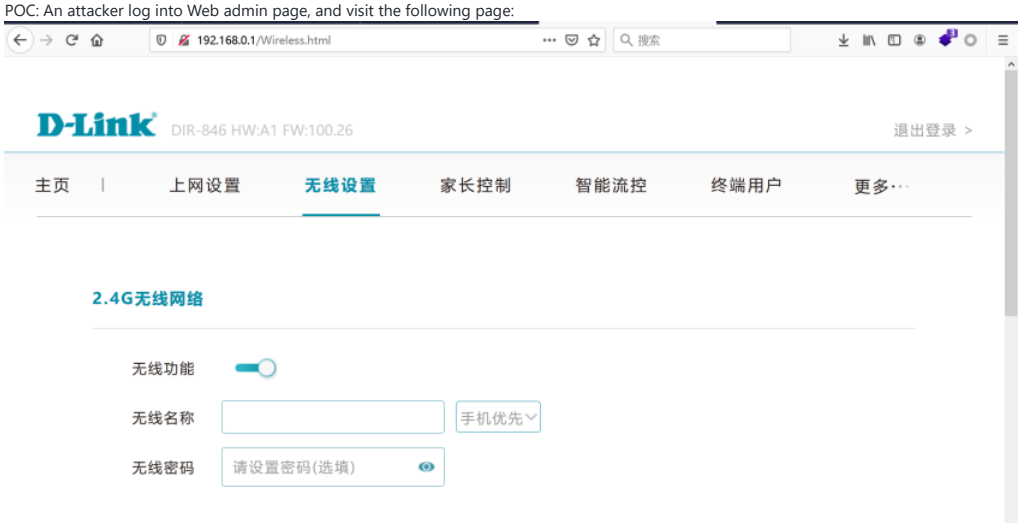
```
                    }else{
                        $val = add_or_update_option_info($val, "wifi-iface\n", '', "encryption",'psk-mixed');
                    }
                    $val = add_or_update_option_info($val, "wifi-iface\n", '', "ssid", $data["ssid1"]);
                    $val = add_or_update_option_info($val, "wifi-iface\n", '', "key", $data["password1"]);
                }elseif(strpos($val,"option ifname 'wlan0'")){
                    $val = add_or_update_option_info($val, "wifi-iface\n", '', "disabled", $data["disabled0"]==1?
                    $set_radio0 = $data["disabled0"]==1?"0":"1";
                    if($option['wl(1).(0)_crypto'] == 'none'){
                        $val = add_or_update_option_info($val, "wifi-iface\n", '', "encryption",'none');
                        //$val = del_option_info($val, "wifi-iface\n", "", "encryption");
                    }else{
                        $val = add_or_update_option_info($val, "wifi-iface\n", '', "encryption",'psk-mixed');
                    }
                    $val = add_or_update_option_info($val, "wifi-iface\n", '', "ssid", $data["ssid0"]);
                    $val = add_or_update_option_info($val, "wifi-iface\n", '', "key", $data["password0"]);
                }
                $wireless_info .= $val;
            }
        }
        if($set_radio1!==false)
            $wireless_info = add_or_update_option_info($wireless_info, "wifi-device", 'radio1', "disabled",$set_r
        if($set_radio0!==false)
            $wireless_info = add_or_update_option_info($wireless_info, "wifi-device", 'radio0', "disabled", $set_

        save_cfg_info("wireless", $wireless_info);
        $unicode_2 = $data["ssid1"];
        exec("ssid_code_set_B2_2_ssid_tmp1 '" . $unicode_2 . "'");
        $unicode_5 = $data["ssid0"];
        exec("ssid_code_set_B5_0_ssid_tmp2 '" . $unicode_5 . "'", $str, $status2);
        // exec("/etc/init.d/network restart");
        exec("ubus call network reload");
        $result["SetMasterWLanSettingsResult"] = "OK";
        $this->api_response(__CLASS__,$result);
    }
```

SetMasterWLanSettings.php

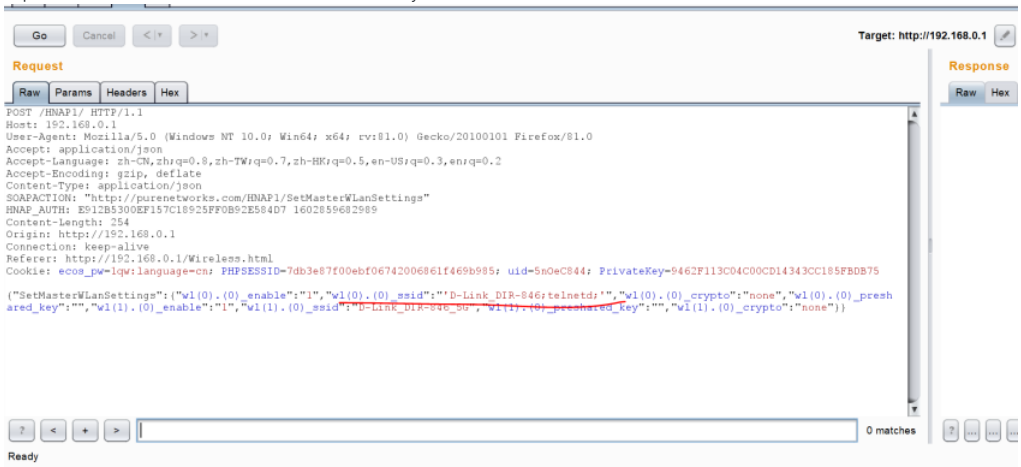
```
<?php
class SetMasterWLanSettings extends GetMultipleHNAPs
{
    function __construct( $act_val){
        parent::__construct( $act_val );
    }
    public function actionIndex(){
        $option = $this->act_val;
        $result["SetMasterWLanSettingsResult"] ="FAIL";
        $data["disabled0"] = intval($option["wl(1).(0)_enable"]);
        $data["ssid0"] = trim($option["wl(1).(0)_ssid"]);
        $data["password0"] = trim(code_decode($option["wl(1).(0)_preshared_key"]));

        $data["disabled1"] = intval($option["wl(0).(0)_enable"]);
        $data["ssid1"] = trim($option["wl(0).(0)_ssid"]);
        $data["password1"] = trim(code_decode($option["wl(0).(0)_preshared_key"]));

        $g_cfg_info = read_cfg_info("wireless");
        if (NULL == $g_cfg_info)
        {
            $this->api_response(__CLASS__,$result);
        }
        if((strlen( $data["ssid0"])==0 || strlen( $data["ssid0"])>60) || strlen( $data["ssid1"])==0 || strlen( $data["ssid1"])>60){
            $this->api_response(__CLASS__,$result);
        }
        if(((!empty($data["password0"]) && strlen($data["password0"])<8) || (!empty($data["password1"]) && strlen( $data["password1"])<8))){
            $this->api_response(__CLASS__,$result);
        }
        $wifi_iface_arr = explode("config wifi-iface\n",$g_cfg_info);
       // $wifi_iface_arr = preg_split("/config.*\n(.*option.*\n)+/", $g_cfg_info);
        $wireless_info = "";
        $set_radio0 = false;$set_radio1 = false;
        foreach($wifi_iface_arr as $key=>$val){
            if(empty($val) || $key==0){
                $wireless_info .= $val;
            }else{
                $val ="config wifi-iface\n".$val;
```

PHP Hypertext Preprocessor file length : 4,334 lines : 79 Ln : 22 Col : 10 Sel : 0 | 0 Windows (CR LF) UTF-8 INS

POC: An attacker log into Web admin page, and visit the following page:



Capture HTTP POST data and edit data to execute arbitrary command such as “telnetd”.



As you can see in the above figure, if an attacker post $data["ssid0"]="'x;telnetd;'" to /HNAP(SetMasterWLanSettings.php), he will open a telnet shell.