Vendor of the products: TP-Link

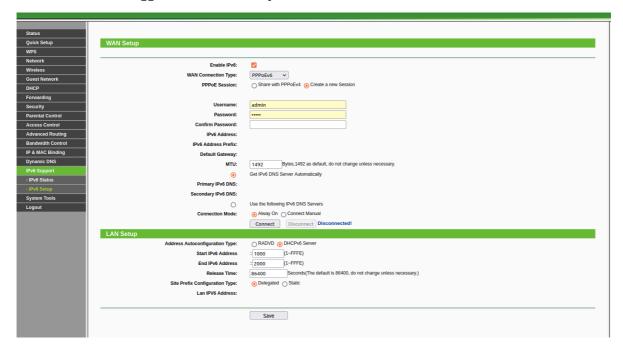
Affected products: TL-WR841ND V11

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 username and password parameters at /userRpm/PPPoEv6CfgRpm.htm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted packet.

The interface that triggers the vulnerability

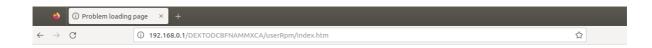


POC

send



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.

Try Again

Similarly, the "password" parameter can also trigger this vulnerability.

send

```
Request

Pretty Raw Hex

© In Second Recognition | Recogni
```

crash

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.

Try Again

Code in httpd

By using IDA to analyze httpd, the program first calls httpGetEnv to retrieve the username and password parameters.

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