

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

The interface that triggers the vulnerability

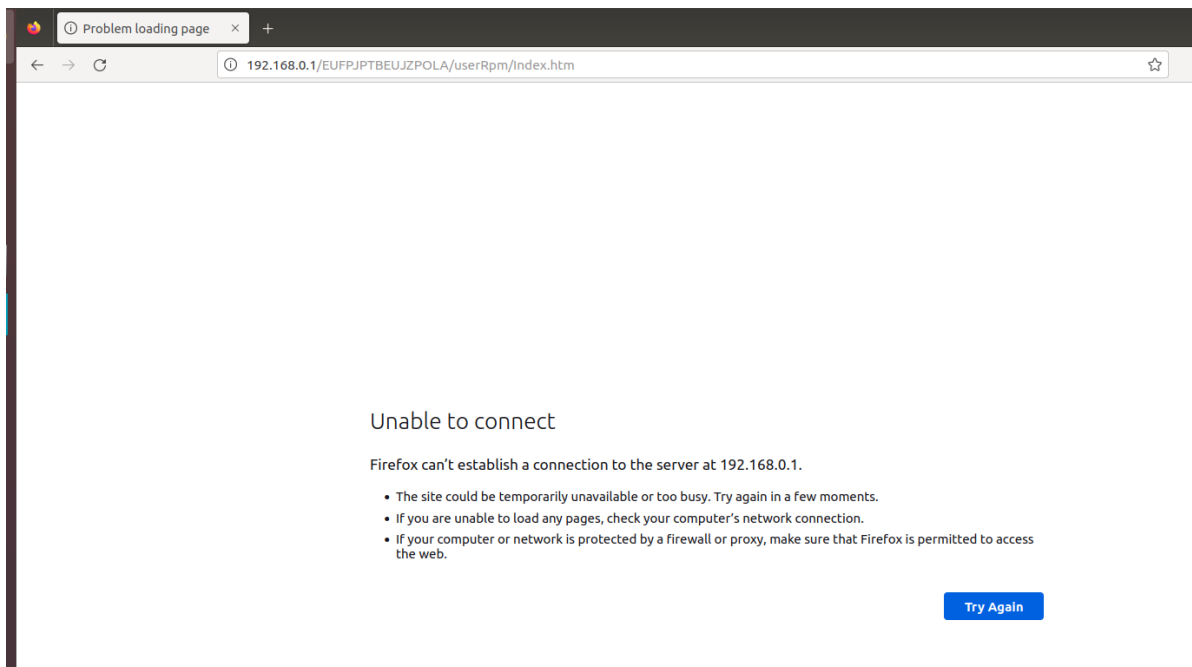
The screenshot shows the TP-Link router's web interface. The left sidebar contains navigation links: Status, Quick Setup, WPS, Network, Wireless (selected), Wireless Settings, Wireless Security, Wireless MAC Filtering, Wireless Advanced, Wireless Statistics, Guest Network, DHCP, Forwarding, Security, Parental Control, Access Control, Advanced Routing, Bandwidth Control, IP & MAC Binding, Dynamic DNS, IPv6 Support, System Tools, and Logout. The main content area is titled 'Wireless Security'. It has three radio buttons: 'Disable Security' (selected), 'WPA/WPA2 - Personal(Recommended)', and 'WPA/WPA2 - Enterprise'. Under 'WPA/WPA2 - Personal', there are dropdowns for 'Version' (WPA2-PSK) and 'Encryption' (AES), a text field for 'Wireless Password' (12345670), and a 'Group Key Update Period' (0 seconds). Under 'WPA/WPA2 - Enterprise', there are dropdowns for 'Version' (Automatic) and 'Encryption' (Automatic), and text fields for 'Radius Server IP', 'Radius Port' (1812), and 'Radius Password'. Under 'WEP', there are dropdowns for 'Type' (Automatic) and 'WEP Key Format' (Hexadecimal), and four 'Key' fields (Key 1 to Key 4) with 'Key Type' dropdowns (all set to 'Disabled'). A 'Save' button is at the bottom.

# POC

send

The screenshot shows a network traffic capture tool with two panels: 'Request' and 'Response'. The 'Request' panel shows a GET request to /EUPFPJTBEUJZPOLA/userRpm/WlanSecurityRpm.htm?pskSecOpt=2&pskCipher=3&pskSecret=12345670&interval=0&secType=2&wpaSecOpt=3&wpaCipher=1&radiusIp=192.168.1.3&radiusPort=1812&radiusSecret=. The 'Response' panel shows a 200 OK status with headers: 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.



## Code in httpd

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

```
225 v38 = (char *)httpGetEnv(a2, "radiusSecret");
226 if ( v38 )
227     goto LABEL_72;
228 if ( v58[2] != 2 || v58[1] != 1 )
229 {
230     v38 = &byte_577C04;
231 LABEL_72:
232     strcpy(&v58[8], v38, v37, v36);
233 }
```

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