Vendor of the products: TP-Link

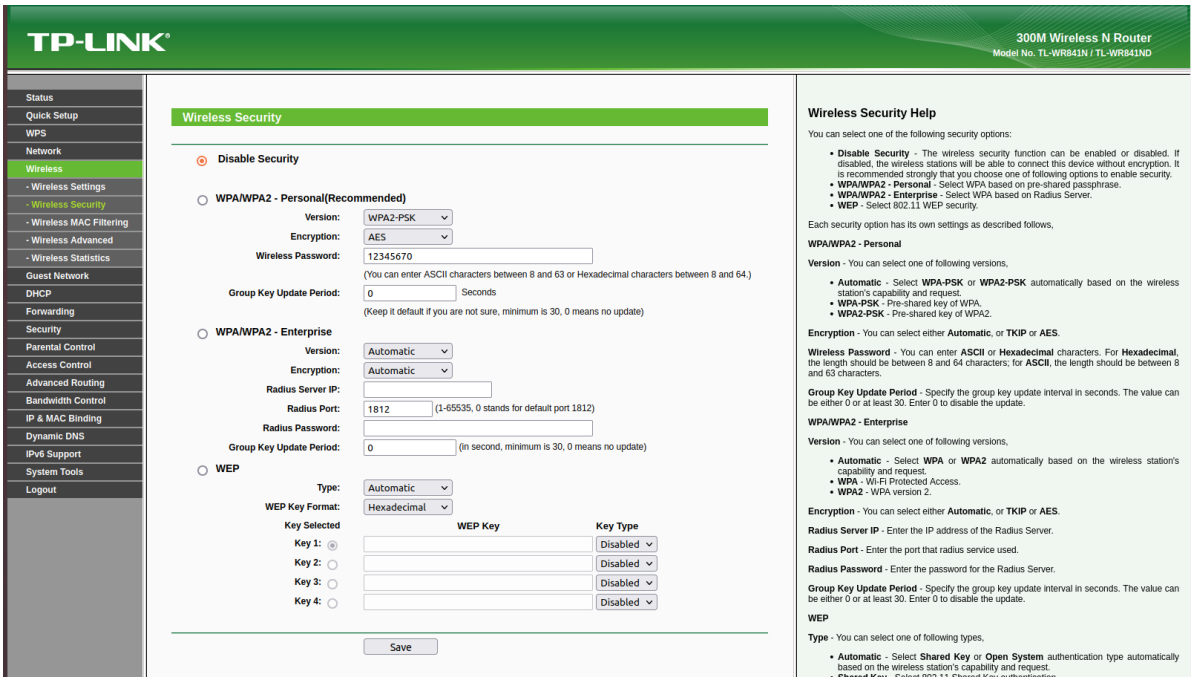
Affected products: TL-WR841ND V11

Hardware Link：https://www.tp-link.com/us/support/download/tl-wr841nd/v11/#Firmware

Vulnerability Description

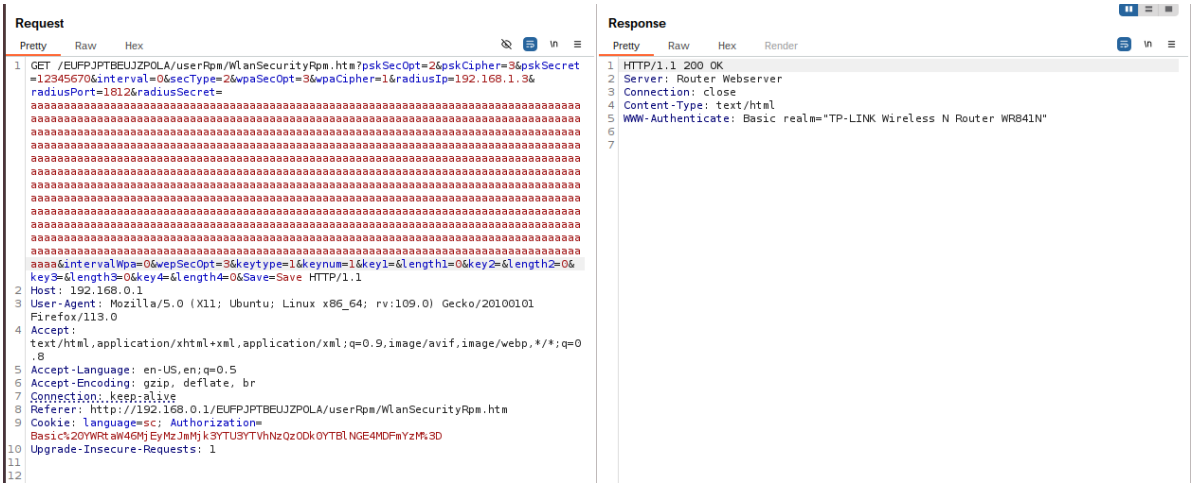
A buffer overflow vulnerability was discovered in TP-Link TL-WR841ND V11, triggered by the pskSecret parameter at /userRpm/WlanSecurityRpm.htm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted packet.

The interface that triggers the vulnerability

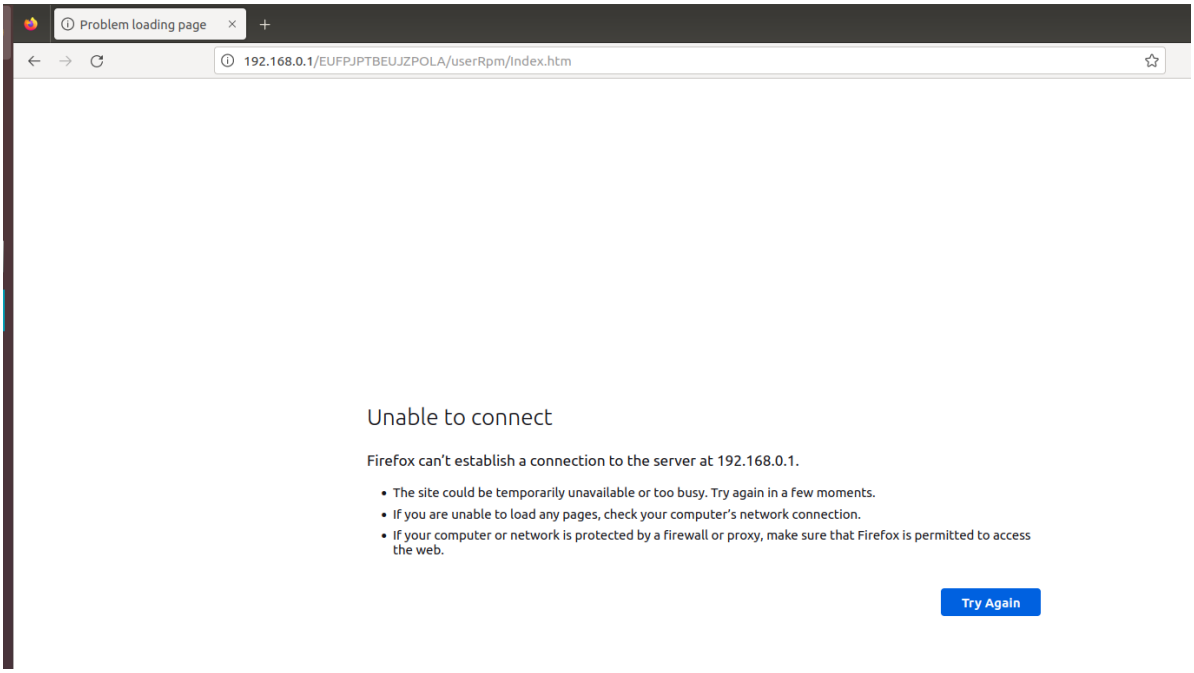


POC

send



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 radiuSecret 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.