TP-Link TL-WR840N V5(EU) and v6.20(EU) UART shell

#TPLINK, #CVE, #UARTSHELL

Last Modified: 2022.05.25.

Advisory

Obtaining root privileges on devices with physical access can be complicated and simple.

A hardware manufacturer is expected to disable hardware debugging interfaces in the end product of commercial products. Unfortunately, many manufacturers do not do this. It would be good to get manufacturers to pay more attention to security.

UART is also one such interface. It is a security issue in itself if it remains enabled. So-called UART shells can be restricted in many ways. It is recommended to set at least password protection.

For a long time, I thought it was not worth reporting such vulnerabilities because in most cases no one cares.

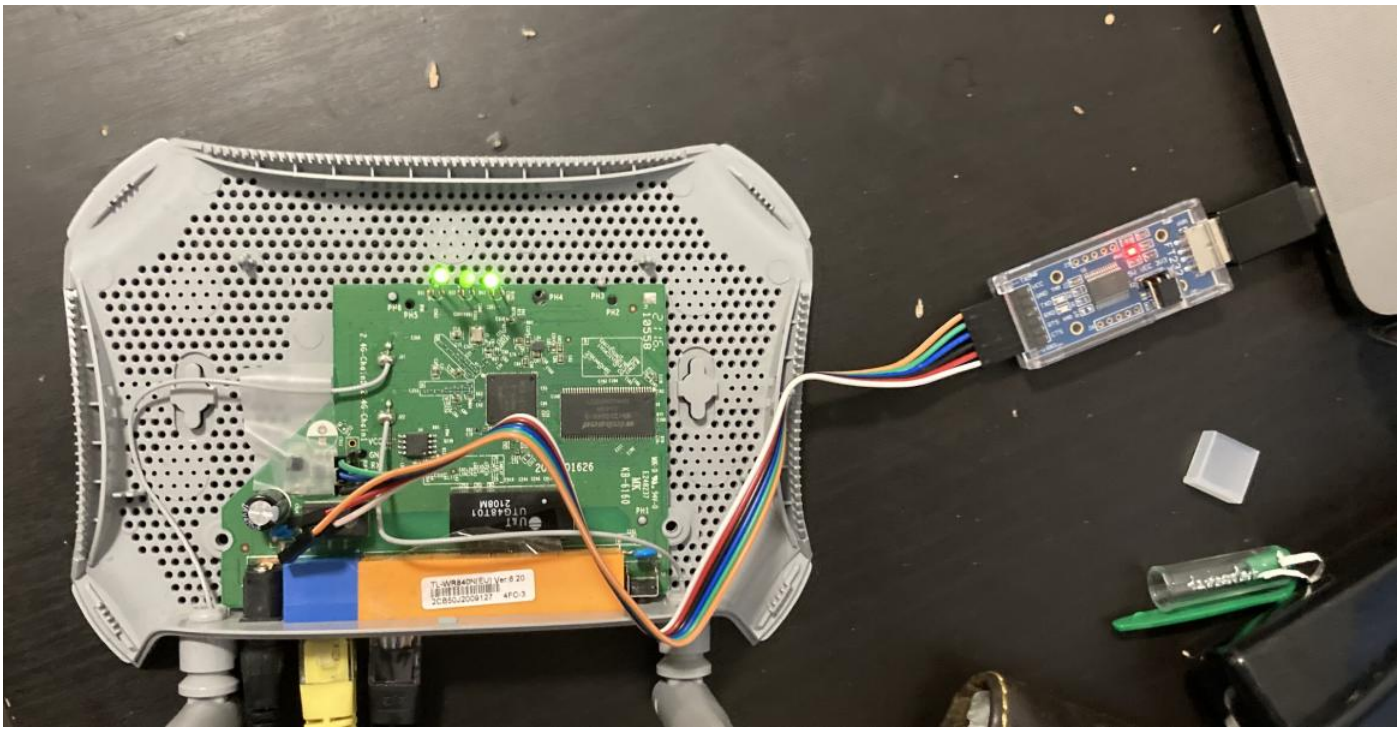
I have noticed that such vulnerabilities in network devices such as routers have recently begun to be reported. (Example: https://nvd.nist.gov/vuln/detail/CVE-2021-23147)

Because the TP-Link TLWR840N EU v6.20 is still available in stores, I have decided to report the vulnerability as well.

TP-Link TLWR840N EU v5/v.620 does not have sufficient protection for the UART console. A malicious actor with physical access to the device is able to connect to the UART port via a serial connection and execute commands as the root user without authentication.

Model: TP-Link TL-WR840N EU v5
Model: TP-Link TL-WR840N EU v6.20

Hardware setup with an FT232 device:



```
# check serial port
screen /dev/tty.usbserial-AB0LR7NH 115200
```

interactive admin/root shell without password:

```
~ # ifconfig eth0
eth0      Link encap:Ethernet  HWaddr C0:06:C3:E2:8B:1C
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:357 errors:0 dropped:0 overruns:0 frame:0
          TX packets:298 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:69606 (67.9 KiB)  TX bytes:87540 (85.4 KiB)
          Interrupt:3

~ # cat /etc/passwd
admin:$1$$iC.dUsGpxNNJGeOm1dFio/:0:0:root:/:/bin/sh
dropbear:x:500:500:dropbear:/var/dropbear:/bin/sh
nobody:*:0:0:nobody:/:/bin/sh
~ # echo $USER
root
~ #
```

Notes

I reported it to the TP-Link security team and as I know they will not fix the issue.

I would like to say thank you to the TP-Link Security Team.

Timeline

It is difficult to say an exact timeline in this case because it has been reported separately along with other vulnerabilities.

- 2021.09.20 - TP-Link Security Team informed about the vulnerability. (v5 case)
- 2021.01.31 - TP-Link Security Team informed about the vulnerability. (v6.20 case)
- 2022.01.15 - TP-Link Security Team sent a response.
- 2022.01.16 - Further discussion.
- 2022.02.15 - Final discussion (TP-Link Security Team, k4m1ll0)
- 2022.04.15 - The advisory published.
- 2022.04.15 - Request new CVE id.
- 2022.05.25 - New CVE id assigned (CVE-2022-29402)