

main

...

CVE\_Request / WiFi-Repeater / WiFi-Repeater\_mb\_wifibasic.assets / WiFi-Repeater\_mb\_wifibasic.md



pghuanghui Add files via upload

History

1 contributor

29 lines (17 sloc) | 937 Bytes

...

## 0x01 Vulnerability description

A vulnerability is in the 'mb\_wifibasic.shtml' page of the Wavlink-WiFi-Repeater,Firmware package version RPTA2-77W.M4300.01.GD.2017Sep19,Visit the constructed page to get the Wi-Fi Basic Setting, and you can set the WiFi at the same time.

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

`http://xxx.xxx.xxx.xxx/mb_wifibasic.shtml`

## 0x02 Affected version

Wavlink-WiFi-Repeater

## 0x03 Vulnerability

This page does not have access permissions set

## 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

WiFi

Basic Settings

2.4G Advanced Settings

AC Advanced Settings

WPS Settings

LAN Settings

IP Address

MAC Address

DHCP Mode

DHCP Server

Settings

Password Settings

Time Zone Settings

Save/Reload Settings

Upgrade Firmware

Information

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

## ← Wi-Fi Basic Setting

Security Type

### 2.4G Wi-Fi Setting

Wi-Fi On/Off ☒ ON ☐ OFF

Wi-Fi SSID

Wi-Fi Key

Wi-Fi Channel

### AC Wi-Fi Setting

On/Off ☐ ON ☒ OFF

Wi-Fi SSID

Wi-Fi Key

Wi-Fi Channel

Apply

Cancel

## 0x05 Acknowledgement

Penwei.Huang