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
```

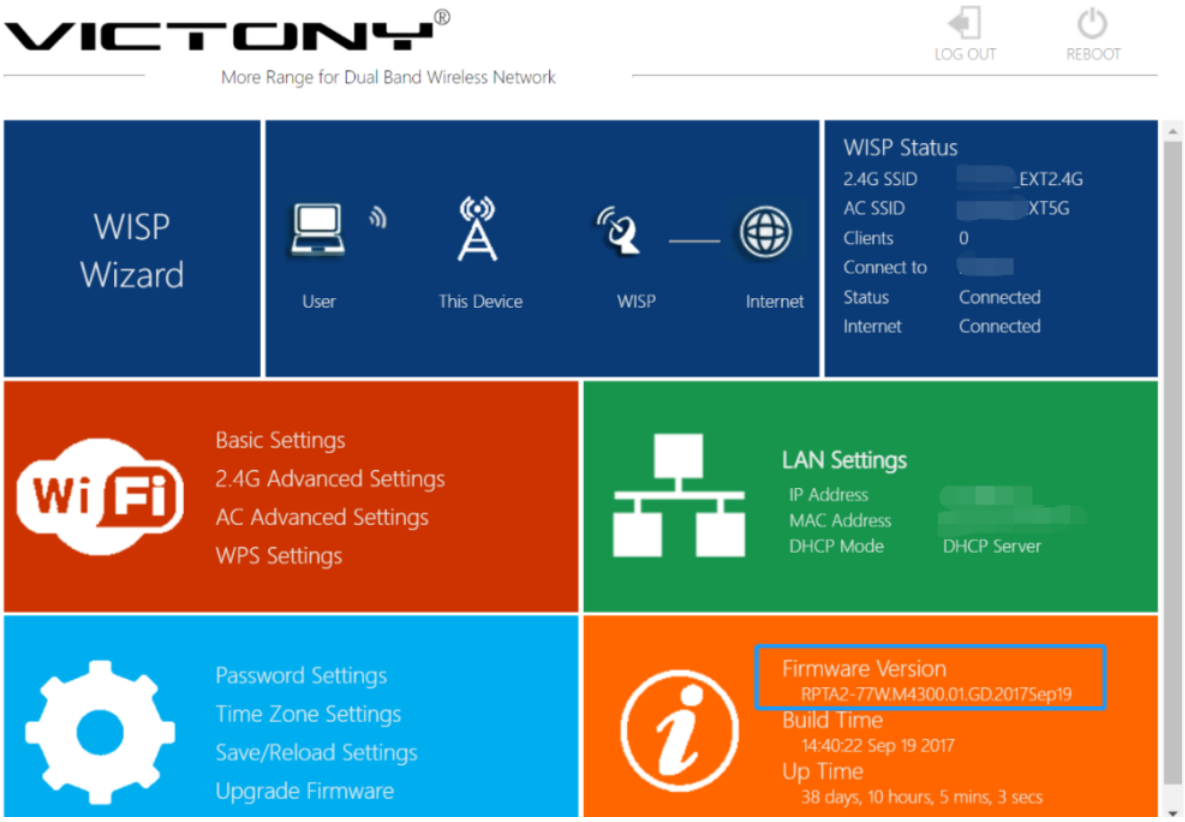
0x02 Affected version

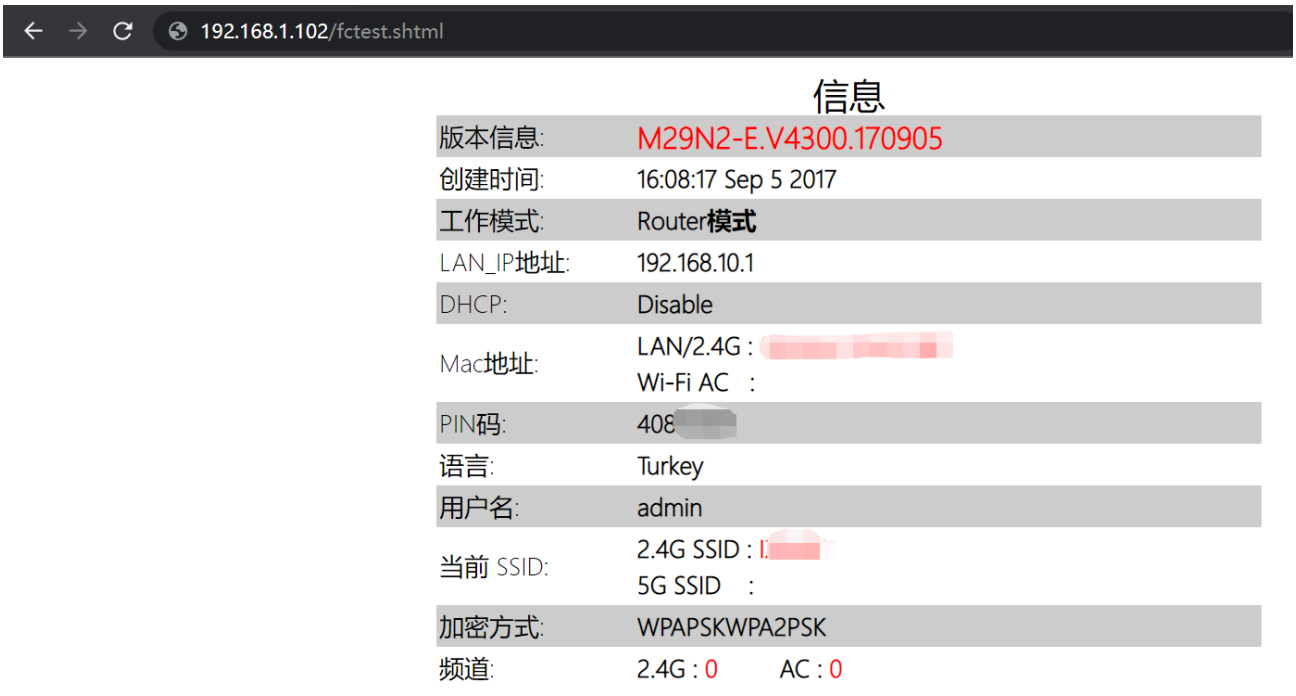
```
Wavlink-WiFi-Repeater
```

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





0x05 Acknowledgement

Penwei.Huang