pghuanghui Add files via upload History

1 contributor

31 lines (18 sloc) | 1.05 KB

0x01 Vulnerability description

A vulnerability is in the 'syslog.shtml' page of the Wavlink-WiFi-Repeater,Firmware package version RPTA2-77W.M4300.01.GD.2017Sep19,Attackers can use this page to configure various functions of the repeater.

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

```
http://xxx.xxx.xxx.xxx/syslog.shtml
```

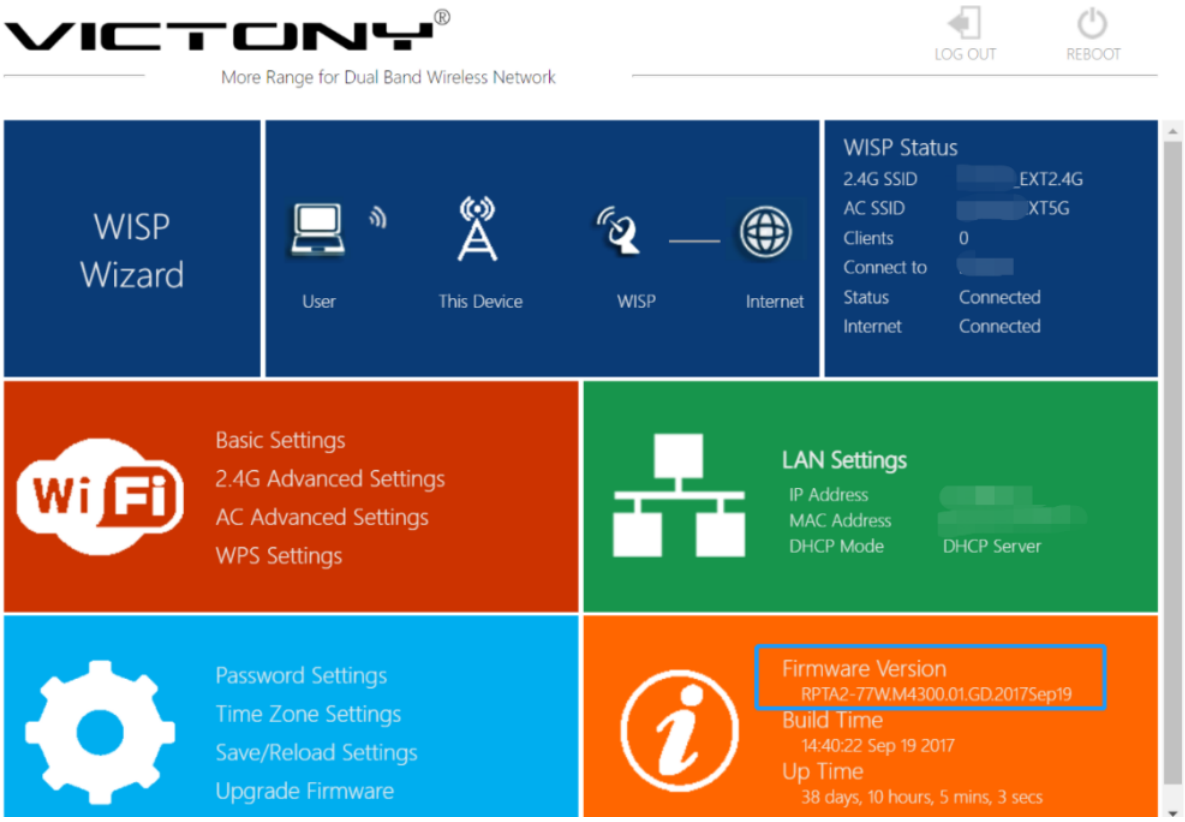
0x02 Affected version

```
Wavlink-WiFi-Repeater
```

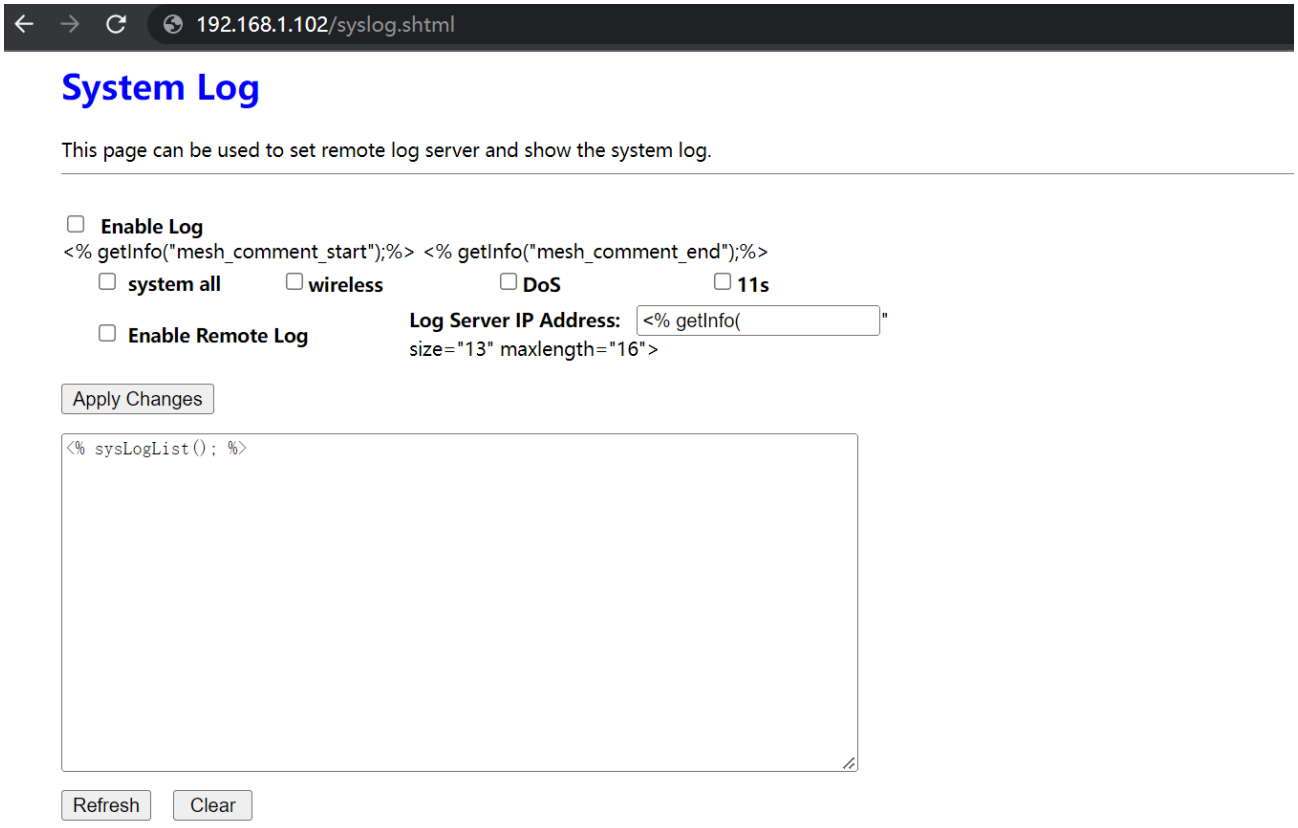
0x03 Vulnerability

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



!(wavlink-WiFi-Repeater_syslog.shtml.assets/image-20220623145655255.png)



0x05 Acknowledgement

Penwei.Huang