pghuanghui Add files via upload History

1 contributor

31 lines (18 sloc) | 1.26 KB

## 0x01 Vulnerability description

An issue was discovered in Wavlink WN579G3,Firmware package version M35G3R.V5030.180927,affecting /cgi-bin/ExportAllSettings.sh where a crafted POST request returns the current configuration of the device, including the administrator password. No authentication is required. The attacker must perform a decryption step, but all decryption information is readily available.

## 0x02 Affected version

```
WAVLINK WN579 G3
```

## 0x03 Vulnerability

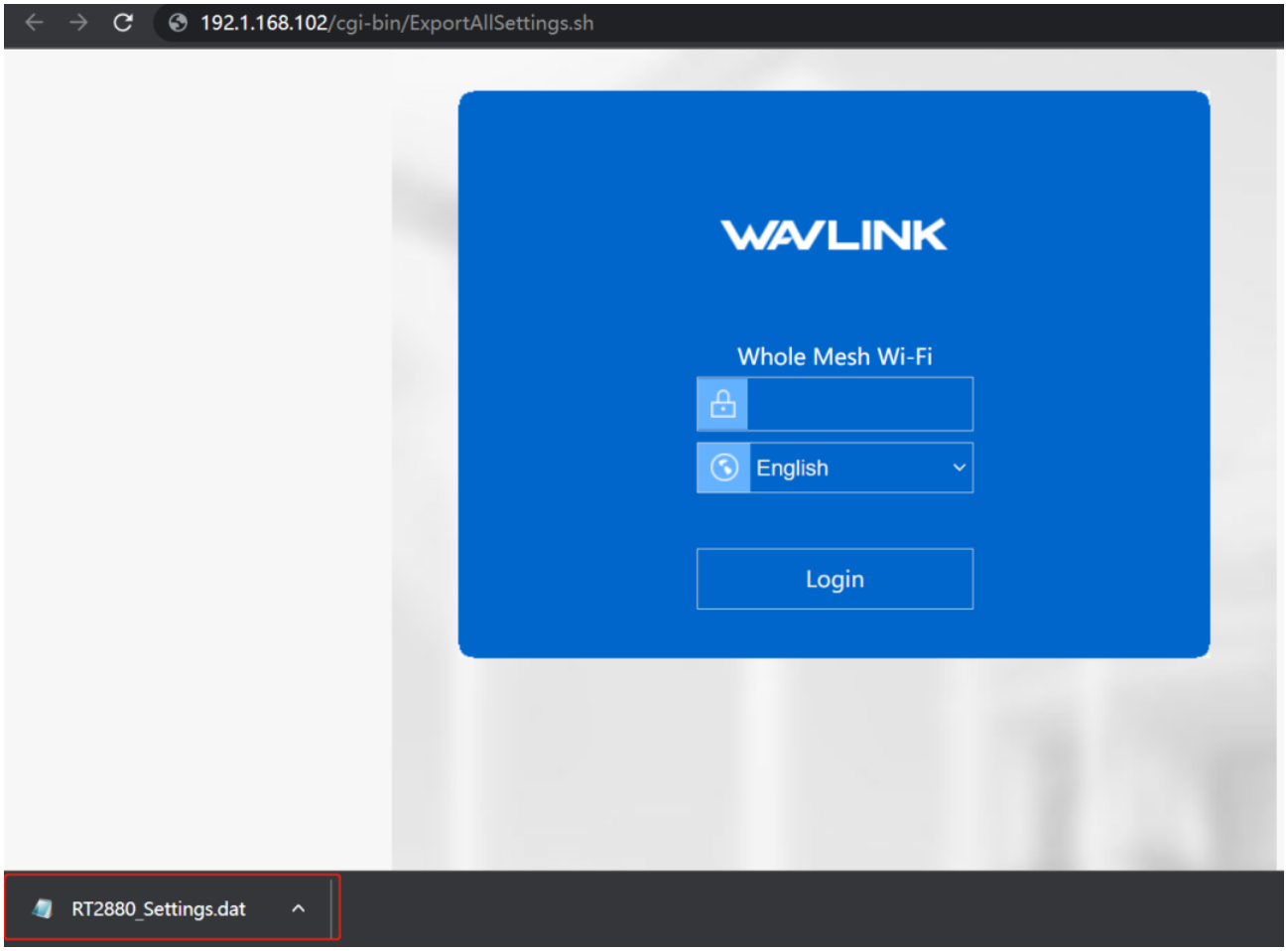
When viewing the /cgi-bin/ExportAllSettings.sh file, it was not properly authorized by the system.

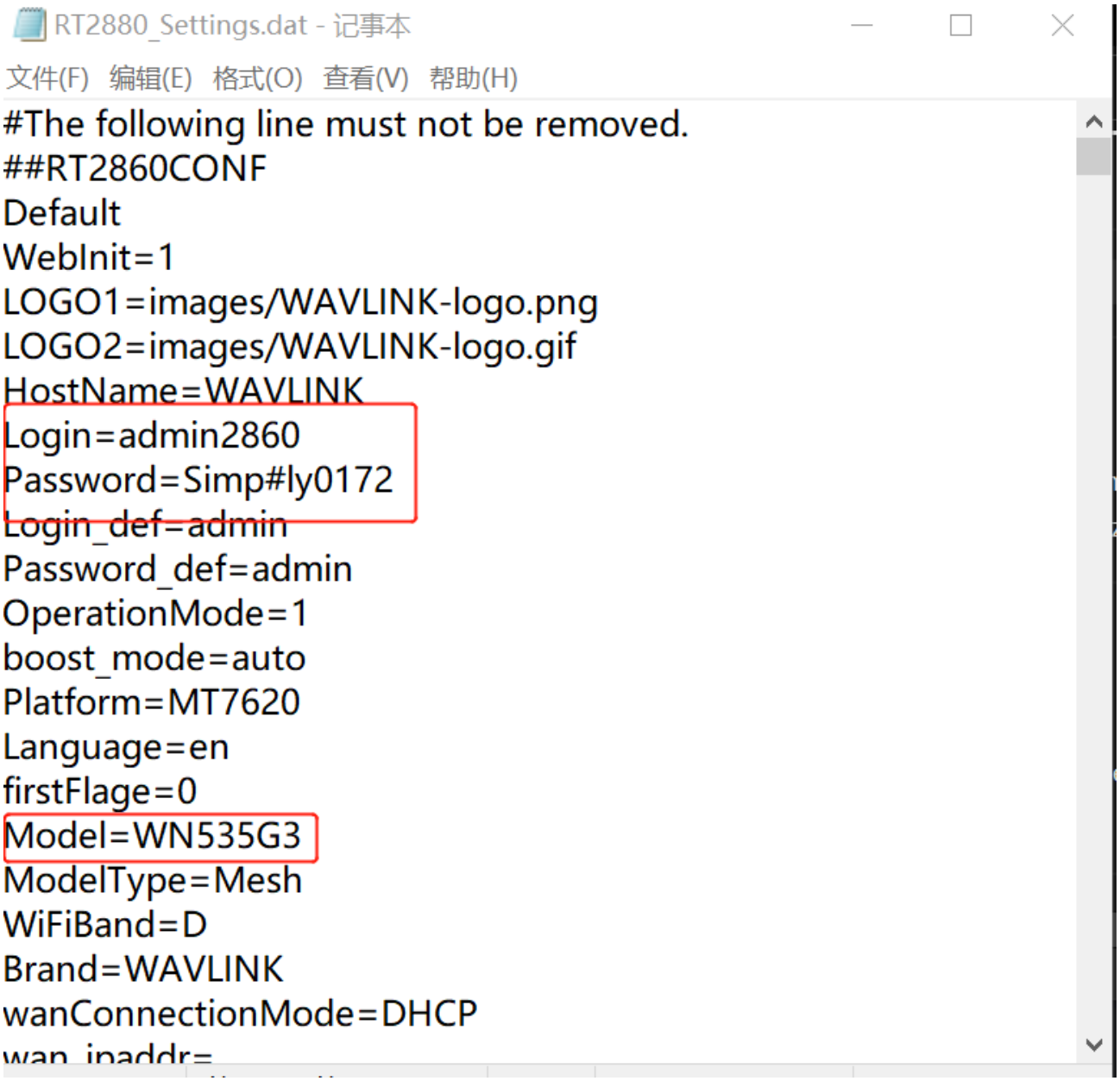
```
function configSave(){
    f=document.frmSetup2;
    f.action="/cgi-bin/ExportAllSettings.sh";
    f.submit() ;
}
```

## 0x04 PoC verification

Directly construct the url link as:

```
http://xxx.xxx.xxx.xxx/cgi-bin/ExportAllSettings.sh
```






## 0x05 Acknowledgement

Penwei.Huang