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

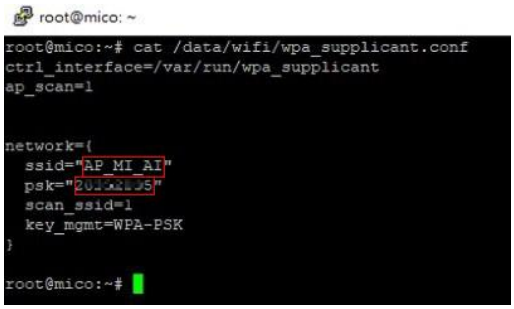

Fig.3 Show the WIFI SSID and password

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

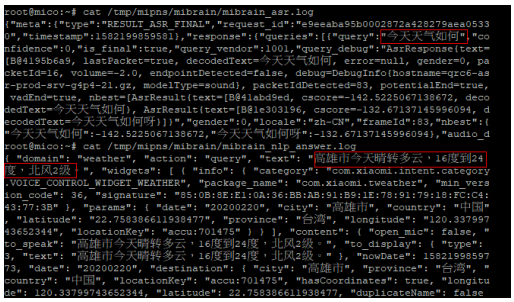

Fig.4 Part of the texts transferred from conversations between the user and XIAOMI XIAOAI speaker Pro

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

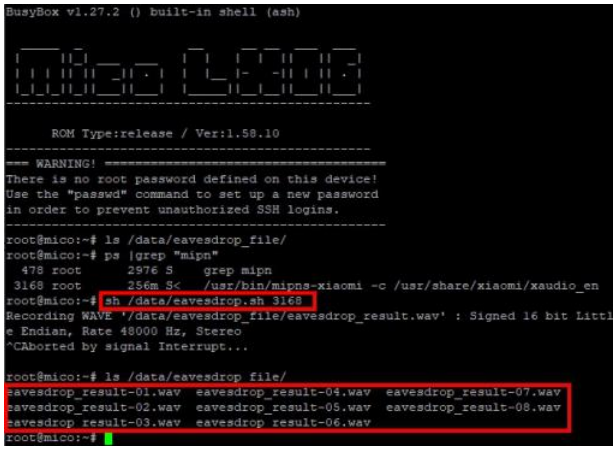

Fig.5 Recording the conversations and show the produced wave files

5. Stop voice assistant service

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

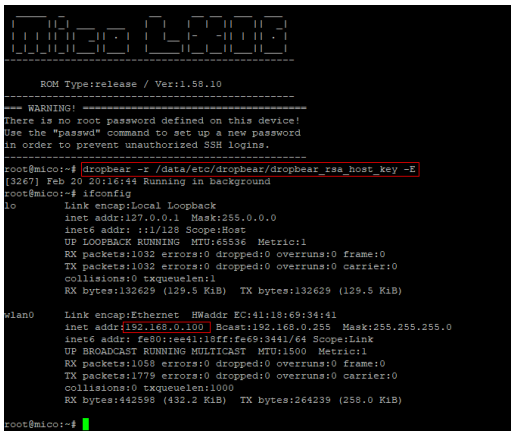

Fig.7 The command to use a RSA format SSH private key

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

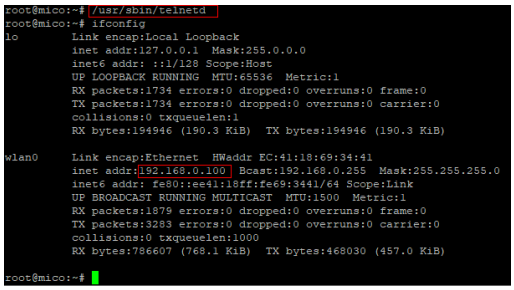

Fig.9 The start Telnet command Fig.

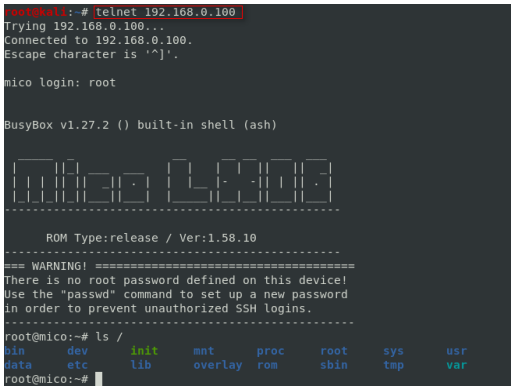

Fig.10 The command to remotely login in by Telnet with no password to be asked.

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

Fig.11 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
66,561,566,561,566,1692,566,561,566,1692,566,1692,566,40349,9004,2242,5
66,95557,9003,2242  >    /sys/ir_tx_gpio/ir_data
root@mico:~#
```

Fig.12 The command to send any IR code

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

Fig.13 The router configuration before data tampering

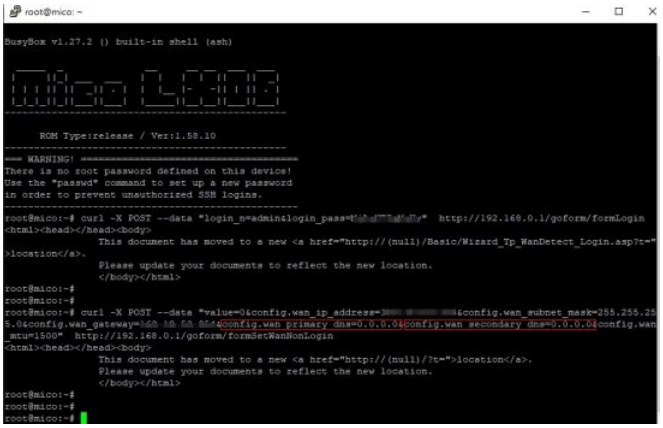

Fig.14 The command for data tampering with the router configuration

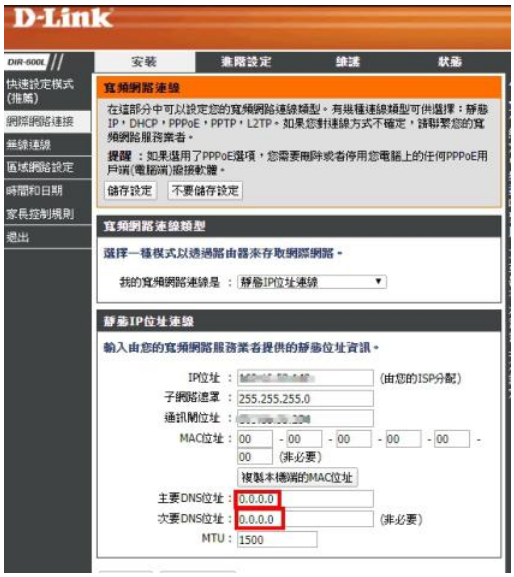

Fig.15 The router configuration after data tampering