CVE-2020-8994

[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 AI speaker MDZ-25-DT 1.34.36, 1.40.14.Attackers can get root shell by accessing the UART interface and then they can read Wi-Fi SSID or password, read the dialogue text files between users and XIAOMI AI speaker, use Text-To-Speech tools pretend XIAOMI speakers' voice achieve social engineering attacks, eavesdrop on users and record what XIAOMI AI speaker hears, delete the entire XIAOMI AI speaker system, modify system files, stop voice assistant service, start the XIAOMI AI speaker's SSH service as a backdoor.

[Attack Type]

Physical

[Product]

XIAOMI AI speaker MDZ-25-DT

[Version]

1.34.36 , 1.40.14

XIAOMI AI speaker MDZ-25-DT devices vulnerability

demonstration

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

Fig.1 A laptop is connected to XIAOMI AI speaker 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 AI speaker MDZ-25-DT devices vulnerability

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

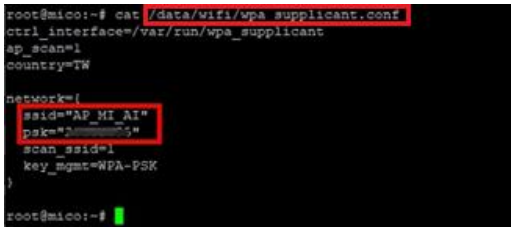

Fig.3 Show the WIFI SSID and password.

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

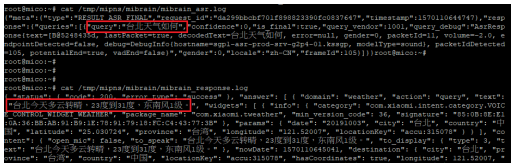

Fig.4 Part of the texts transferred from conversations between the user and XIAOMI AI speaker

3. Use Text-To-Speech tools pretend XIAOMI speakers' voice achieve social engineering attacks

video：https://youtu.be/yCadG38yZW8

4. Eavesdrop on users and record what XIAOMI AI speaker hears

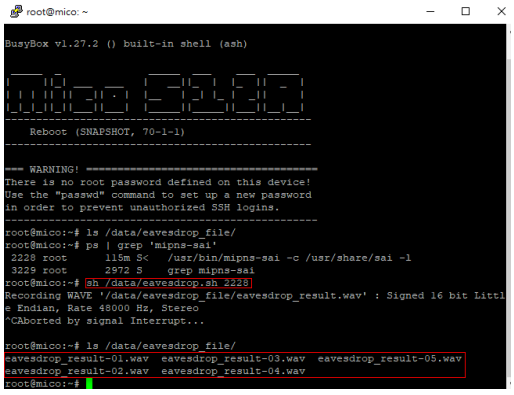

Fig.5 Recording the conversations and show the produced wave files.

5. Delete the entire XIAOMI AI speaker system

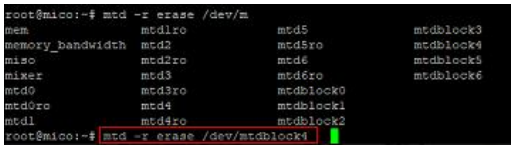

Fig.6 The command to erase the entire speaker system.

6. Stop voice assistant service

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

7. Start the XIAOMI AI speaker's SSH service as a backdoor

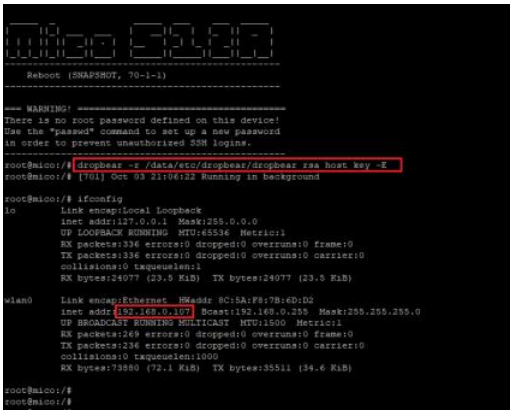

Fig.8 The command to use a RSA format SSH private key.

Fig.9 The command to remotely login in by SSH with no password to be asked.