# CVE Detail – CVE-2020-10263

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.

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## EPSS

EPSS Score: N/A

Percentile: 0.3436

## CVSS Scoring

CVSS v3.1 Score: 6.8

Severity: MEDIUM

## Mapped CWE(s)

* CWE-306: Missing Authentication for Critical Function

## CAPEC(s)

* CAPEC-12: Choosing Message Identifier
* CAPEC-166: Force the System to Reset Values
* CAPEC-216: Communication Channel Manipulation
* CAPEC-36: Using Unpublished Interfaces or Functionality
* CAPEC-62: Cross Site Request Forgery

## Affected Products

* cpe:2.3:o:mi:xiaomi\_xiaoai\_speaker\_pro\_lx06\_firmware:1.52.4:\*:\*:\*:\*:\*:\*:\*