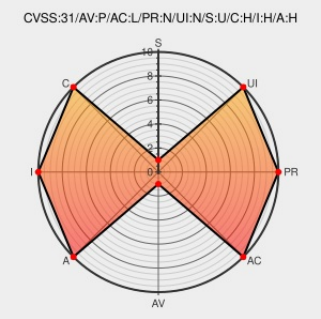
# CVE-2020-10262

Published on: 04/08/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

## CVE-2020-10262

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Xiaomi Xiaoai Speaker Pro Lx06 from Mi contain the following vulnerability:

An issue was discovered on XIAOMI XIAOAI speaker Pro LX06 1.58.10. Attackers can activate the failsafe mode during the boot process, and use the mi_console command cascaded by the SN code shown on the product to get the root shell password, and then the attacker 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's SSH or TELNET service as a backdoor, (IX) tamper with the router configuration of the router in the local area networks.

CVE-2020-10262 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

### CVSS3 Score: 6.8 - MEDIUM

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| PHYSICAL | LOW | NONE | NONE |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| UNCHANGED | HIGH | HIGH | HIGH |

### CVSS2 Score: 7.2 - HIGH

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| LOCAL | LOW | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |

| COMPLETE | COMPLETE | COMPLETE |
|---|---|---|

## CVE References

| Description | Tags | Link |
|---|---|---|
| 小米安全中心 | Vendor Advisory<br>sec.xiaomi.com<br>text/html | MISC sec.xiaomi.com |
| CVE-POC/CVE-2020-10262.md at master · Jian-Xian/CVE-POC · GitHub | Exploit<br>Third Party Advisory<br>github.com<br>text/html | MISC github.com/Jian-Xian/CVE-POC/blob/master/CVE-2020-10262.md |
| XIAOMI XIAOAI speaker Pro' voice achieve social engineering attacks - YouTube | Exploit<br>Third Party Advisory<br>www.youtube.com<br>text/html | MISC www.youtube.com/watch?v=Cr5DupGxmL4 |



There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Hardware | Mi | Xiaomi Xiaoai Speaker Pro Lx06 | - | All | All | All |
| Hardware | Mi | Xiaomi Xiaoai Speaker Pro Lx06 | - | All | All | All |
| Operating System | Mi | Xiaomi Xiaoai Speaker Pro Lx06 Firmware | 1.58.10 | All | All | All |
| Operating System | Mi | Xiaomi Xiaoai Speaker Pro Lx06 Firmware | 1.58.10 | All | All | All |

cpe:2.3:h:mi:xiaomi_xiaoai_speaker_pro_lx06:-:*:*:*:*:*:*:*:

cpe:2.3:h:mi:xiaomi_xiaoai_speaker_pro_lx06:-:*:*:*:*:*:*:*:

cpe:2.3:o:mi:xiaomi_xiaoai_speaker_pro_lx06_firmware:1.58.10:*:*:*:*:*:*:*:

cpe:2.3:o:mi:xiaomi_xiaoai_speaker_pro_lx06_firmware:1.58.10:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

**CVE.report and Source URL Uptime Status status.cve.report**