



CVE-2020-10262

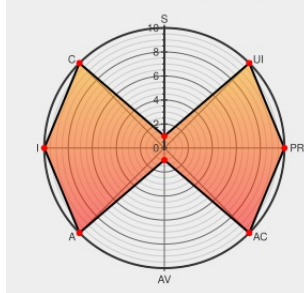
Published on: 04/08/2020 12:00:00 AM UTC

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

CVE-2020-10262

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



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 [M](#) 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 sec.xiaomi.com text/html	 MISC sec.xiaomi.com
CVE-POC/CVE-2020-10262.md at master · Jian-Xian/CVE-POC · GitHub	Exploit Third Party Advisory github.com 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 Third Party Advisory www.youtube.com text/html	 MISC www.youtube.com/watch?v=Cr5DupGxmL4

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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 →](#)

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)