YEALINK YEACAST & PA20

SUMMARY REPORT

19 May 2025

EXECUTIVE SUMMARY

Context and Scope

This report describes the results of the security evaluation of the Yealink PA20 and Yealink YeaCast performed by Kudelski IoT Security Laboratories in Cheseaux-sur-Lausanne, Switzerland, between March 11th and March 21st.

The goal of the engagement was to evaluate the overall security level of the Yealink YeaCast software and the communications between the PA20 and an endpoint.

Main Outcomes and Recommendations

Kudelski Laboratories performed a security evaluation of the Yealink PA20 and Yealink YeaCast to assess the overall security level of the Yealink YeaCast software and the communications between the PA20 and an endpoint.

During this timebound exercise performed on latest firmware version 270.357.0.4, no security risk could be evidenced, either during device mounting and pairing or user to endpoint connection and communication.

Identified Strengths

ID	TESTED PROCESS	DESCRIPTION
S01	Device mounting	The CD-ROM / mass storage exposed by the PA20 is in read-only access, preventing from undesired software modifications.
S02	Communication	A secure connection is established between the YeaCast end user and the endpoint.
S03	Connection	Enabling the BYOD mode is requiring a user confirmation on the endpoint.
S04	Device pairing	The Wi-Fi AP SSID and password are transmitted encrypted or obfuscated to the PA20 dongle during its pairing.