TestArmy Group S.A. has carried out Hardware Penetration Test of AudioCodes Limited devices - the RXV200 intelligent AV hub and the RX-PAD room controller. The objective of these penetration tests was to evaluate the current security status of the provided devices and the related applications by identifying issues that could adversely affect confidentiality, integrity, or availability.

The security tests were conducted in accordance with the OWASP MASVS v.2.1.0 testing methodology (https://www.owasp.org/) and the OWASP Mobile Security Testing Guide and OWASP Mobile Top 10 for 2024. Using a combination of automated tools and manual penetration testing process, TestArmy Group S.A penetration testers attempt to detect vulnerabilities using the techniques, tools and crafted exploit scripts that are similar to those used by attackers.

The following vulnerabilities were specifically examined: analysis of application architecture and design, analysis of data storage and privacy, cryptographic analysis, analysis of the authentication process and session management, analysis of network communication (verification whether confidentiality and integrity of information exchanged between the mobile application and remote service endpoints is ensured), mobile application verification (application must provide a secure, encrypted network communication channel using SSL / TLS with appropriate settings), analysis of used APIs and standard application components, analysis of the means of protection used (application resistance to reverse engineering and customer attacks).

The first iteration of the Penetration test was performed between 12.08.2025 and 20.08.2025.

The first iteration of the penetration test and security retest were performed for the following device models and associated firmware and embedded applications:

TEST MODEL	Software version
AudioCodes RX-PAD	V 3.0.9
AudioCodes RXV200	V 3.0.9

During the verification process, the detected security vulnerabilities from the first iteration of the pentest have the following status:

VULNERABILITY SEVERITY	Quantity	**Vulnerability name**
Critical	0	0
High	0	0
Medium	1	Firmware updates retrieved via unencrypted channels
Low	2	Exported WebView activity susceptible to abuse Insecure WebView implementation increasing attack surface