



December 6, 2022

To whom it may concern:

As part of Yealink Inc.'s ongoing commitment to ensuring the security and integrity of its systems and data, Yealink Inc. engaged NetSPI to perform an Embedded Device Penetration Test against the MeetingBoard 65. The purpose of this penetration test was to identify common security issues that could adversely affect the confidentiality, integrity, or availability of the application, the device, and related data.

NetSPI security consultants follow a phased assessment approach for testing the security of applications and devices. NetSPI consultants use multiple commercial and open source security tools, custom scripts, and manual techniques to scan for, identify, and exploit vulnerabilities within applications.

NetSPI uses a combination of automated tools and manual penetration testing processes to identify missing, broken, and improperly used application security controls. NetSPI security consultants attempt to penetrate or circumvent existing security mechanisms by using tools, exploit scripts, and techniques that are similar to those used by attackers. The testing targets common vulnerabilities, including the OWASP Top Ten (<http://www.owasp.org>) and other flaws typical of similar applications. In this manner, our approach analyzes the current security posture and results in recommendations for strengthening security controls.

The initial testing was concluded on September 6, 2022. Remediation testing of high and medium severity vulnerabilities was performed between November 11, 2022 and November 18, 2022.

Initial and remediation testing and verification was performed against the following device, associated firmware, and embedded application:

PRODUCT SERIES	TEST MODEL	FIRMWARE VERSION (INITIAL TEST)	FIRMWARE VERSION (REMEDIATION TEST)
MeetingBoard 65 and MeetingBoard 86	MeetingBoard 65	155.15.0.8	155.15.0.17

NetSPI determined the below remediation status for each vulnerability:

SEVERITY	REMEDIATION STATUS
High	Remediated
Medium	Remediated
Low	Planned Fix

Sincerely,
Charles Horton
SVP of Services