November 2, 2020
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 a Hardware Penetration Test. 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 and verification was performed between June 29, 2020 and July 17, 2020. Remediation testing of high and medium severity findings was performed on September 8, 2020 and October 1, 2020. Per the statement of work, no remediation testing was conducted on low severity vulnerabilities.

Initial and remediation testing was performed against the following devices, associated firmware, and embedded applications:

PRODUCT SERIES	TEST MODEL	FIRMWARE VERSION (INITIAL TESTING)	FIRMWARE VERSION (REMEDIATION TESTING)
MP54 / MP56 / MP58	MP56	122.15.0.9	122.15.0.17
T55A / T56A / T58A / CP960	T58A	58.15.0.104	58.15.0.112
VC210 / A20 / A30	VC210	118.15.0.19	118.15.0.34

Through a process of post-remediation testing concluded on October 1, 2020, NetSPI determined the below remediation status for each vulnerability:

VULNERABILITY SEVERITY	INITIAL TESTING	REMEDIATION TESTING VULNERABILITY STATUS			
		REMEDIATED	PARTIALLY REMEDIATED	NOT REMEDIATED	NOT TESTED
High	7	7	0	0	0
Medium	8	6	1	1	0
Low	9	0	0	0	9

For the two medium severity vulnerabilities that were found during NetSPI's remediation testing to either be partially remediated or not remediated, Yealink has attested that the fixes have been developed and will be deployed in the next release. For the low severity vulnerabilities that were not in-scope for remediation testing as a part of the statement of work between NetSPI and Yealink, Yealink has attested that they have implemented fixes in accordance with NetSPI's recommendations.

Sincerely,
Charles Horton
VP of Services