NETSPI

Embedded Penetration Test

Executive Summary

Project: DeskVision A24

Yealink

December 28, 2023

Contents

Chapter 1 | Project Summary

NetSPI performed an analysis of Yealink (Xiamen) Network Technology CO., Ltd's (Yealink) DeskVision A24 device to identify vulnerabilities, determine the level of risk they present to Yealink, and provide actionable recommendations to reduce this risk. NetSPI compiled this report to provide Yealink with detailed information on each vulnerability discovered within the DeskVision A24 device, including potential business impacts and specific remediation instructions.

1.1 Project Objectives

NetSPI's primary goal within this project was to provide Yealink with an understanding of the current level of security in the device and its infrastructure components.

NetSPI completed the following objectives to accomplish this goal:

- Identifying application-based threats to and vulnerabilities in the device and application
- Identifying network-based threats to and vulnerabilities in the device
- Identifying hardware-based threats to and vulnerabilities in the device
- Comparing Yealink's current security measures with industry best practices
- Providing recommendations that Yealink can implement to mitigate threats and vulnerabilities and meet industry best practices

1.2 Scope & Timeframe

Testing and verification was performed between November 6, 2023 and November 13, 2023. The scope of this project was limited to the following devices, associated firmware, and embedded applications.

PRODUCT SERIES	TEST MODEL	FIRMWARE VERSION
DeskVision	A24	156.15.0.21

NetSPI conducted the tests using production version of the devices. All other applications and servers were out of scope. All testing and verification was conducted from outside of Yealink's offices.

1.3 Summary of Findings

NetSPI's assessment of the DeskVision A24 device revealed the following vulnerabilities:

- 1 informational severity vulnerability

VULNERABILITY NAME	SEVERITY
Unsupported Version – Android 10	Informational

TABLE 1: FINDINGS SUMMARY

1.4 Network Geolocation Audit

At the request of Yealink, NetSPI audited the network traffic of the device during the firmware upgrade process as well as normal operation looking for traffic to hostnames or IP addresses which geolocate within the People's Republic of China. No such traffic was discovered.