KSIZPE LED Strip Light Security Analysis Report

Preston Chapman

Keven Baquerizo

University of Advancing Technology

NTW233

Dr. Becote

Executive Summary

This report presents a comprehensive security analysis of our chosen device, the KSIPZE 100ft LED Strip Lights, a budget-friendly consumer IoT device. Our findings synthesize prior research into the device's hardware, wireless communication, application, and potential attack vectors. We discovered several vulnerabilities, including weak or zero authentication, lack of encryption, undocumented firmware update processes, and exposed hardware interfaces. These weaknesses expose end-users to risks such as unauthorized control, privacy breaches, and data exfiltration. Recommendations are provided for the manufacturer to improve hardware design, firmware protections, and application security.

Introduction

The KSIPZE 100ft LED Strip Lights are a popular smart decorative lighting designed for consumers to use them however they want to, home use being to most common use. Although users can control the device using an Infrared Remote, it is also marketed as being compatible with smartphone apps using Bluetooth, and Wi-Fi. The device provides RGB lighting, music synchronization, scheduling, and room synchronization features. However, as a budget product, the manufacturer's focus appears to be on affordability rather than having robust security in mind, something that was proven during this security analysis.

Scope of Analysis

We have conducted several analysis and inspections of our chosen device, such as visual inspection, disassembly, wireless traffic analysis, firmware inspection, and research of the mobile application. The goal was to uncover security vulnerabilities and recommend mitigations following frameworks such as STRIDE, OWASP IoT and NIST CSF.

Methodology

- Environmental scanning of product manuals and FCC filings.
- Threat modeling using STRIDE.
- Hardware teardown and component identification.
- Wireless and Bluetooth pairing tests.
- App functionality assessment.

Device Details

- **Manufacturer:** KSIPZE
- **Model:** ST51_K2430
- **Form Factor:** Controller box + LED strips + IR remote + 24V adapter
- **Key Features:** RGB control, music sync, scheduling, app-based configuration
- **Connectivity:** Advertised Bluetooth and 2.4GHz Wi-Fi (only Bluetooth confirmed functional)
- **Control App:** "Happy Lighting" (Android/iOS)
- **Hardware Components Identified:**
    - Microcontroller (unbranded, low-end SoC)
    - Voltage regulators (24V to 3.3V step-down)
    - IR receiver, microphone, PCB antenna
    - JST connectors to LED strips

  - S8050 transistors, current-limiting resistors

Intended Functionality

This device is a RGB light strip, allowing it to change from assorted colors, the strip is adhesive and one hundred feet long, it will use a standard infrared remote that has controls such as brightness, colors, timers, presets, and animations. The user can also download the compatible app “Happy Lighting,” where the user can then control the device using their phone.

Threat Model

Identified Threats (STRIDE):

- **Spoofing:** Unauthenticated Bluetooth connections allow any nearby actor to assume control.
- **Tampering:** Debug pads and open IR interface can be exploited to inject malicious commands.
- **Repudiation:** No audit logs or authentication records make attribution impossible.
- **Information Disclosure:** Bluetooth traffic appears unencrypted, exposing sensitive signals.
- **Denial of Service:** IR floods, Bluetooth jamming, or power surges could disable operation.
- **Elevation of Privilege:** If firmware update pathways are unprotected, attackers may escalate privileges with malicious firmware.

Impact:

- Unauthorized users could hijack lighting control, invade privacy via microphone, or pivot to other devices on the same network.
- In public settings (venues, dorms), devices can be easily exploited for nuisance or malicious behavior.

For a full report of the Threat Model of the RGB light strips, please view the following document: Security Assessment Framework.docx

Firmware Analysis

- No official firmware files were identified from the manufacturer’s site or app store.
- App-based update capability is advertised but no changelogs or signatures are visible.
- **Risks:**
  - Firmware may contain hardcoded keys or outdated libraries.
  - Without signed updates, malicious firmware could be sideloaded.

Smartphone Application Analysis

- **App:** “Happy Lighting” (Android/iOS)
- **Findings:**
  - No authentication required for pairing.
  - Permissions request includes unnecessary access such as location data.
  - No evidence of end-to-end encryption between app and device.
- **Risks:**

  - Users' privacy compromised by excessive permissions.
  - Lack of secure pairing enables unauthorized control.

Wi-Fi Traffic Analysis

- Despite marketing claims, Wi-Fi pairing attempts failed.
- Hypothesis: This model may lack Wi-Fi hardware, or firmware disables it.
- Risks**:** If enabled in other variants, Wi-Fi without WPA2/3 security could leak unencrypted commands and metadata.

Hardware Analysis

Visual Inspection Findings:

- DC power input, antenna, IR receiver, microphone, JST LED connectors.
- Missing protections: no seals, shielding, or tamper evidence.
- Test pads may expose UART/SWD debugging.

Disassembly Findings:

- Microcontroller manages LED logic, connected to SMD crystal for clock.
- Regulators and transistors manage power and LED channel driving.
- IR sensor and mic expose secondary attack surfaces.
- No secure boot or cryptographic chips were detected.

Hardware Vulnerabilities:

- Open IR channel can be spoofed with universal remotes.

- Debug pads may allow firmware extraction.
- Always-on Bluetooth broadens attack window.

For a full report of the Hardware Analysis of the RGB light strips, please view the following document: Hardware Analysis of KSIZPE LED Strip Light.pdf

Recommendations for Mitigations

Firmware/Software Level:

- Implement signed firmware updates with integrity checks.
- Require secure Bluetooth pairing with passkeys or numeric comparison.
- Encryption of Bluetooth traffic (AES-128 or higher).
- Limit app permissions (remove unnecessary location access).

Hardware Level:

- Disable debug/test pads in production firmware.
- Add tamper-evident seals to casing.
- Shield antenna/IR receiver to limit signal leakage.
- Add fuse and TVS protection to power input.

User-Level Best Practices:

- Disconnect when not in use.
- Avoid usage in public or shared environments.
- Use devices on isolated VLANs or guest networks.

Recommendations for Further Research

- Conduct penetration testing on the BLE stack using tools like GATTacker.
- Perform static/dynamic analysis on the "Happy Lighting" APK for hidden API calls.
- Investigate whether Wi-Fi chip is present but disabled (FCC filings).
- Explore potential bi-directional data collection (mic monitoring, telemetry).

Conclusion

The KSIPZE 100ft LED Strip Lights demonstrate significant gaps in IoT security, reflecting the risks common in budget friendly consumer electronics. While it is functional and popular, the device exposes users to unauthorized access and privacy concerns due to weak authentication, lack of encryption, and poor documentation. Implementing the recommended mitigations would raise the device to minimum industry security standards, keep consumers safe, and help restore consumer trust.

Documents

- NTW233 Final IoT Device Security Analysis Report
- Security Assessment Framework.docx
- Hardware Analysis of KSIZPE LED Strip Light.pdf
- IoT Security Analysis Report Draft.pdf

References

Amazon.com product listing: KSIPZE 100ft LED Strip Lights

Aexit HT7533-1 Voltage Regulator: https://www.amazon.com/Aexit-HT7533-1-Package-Regulator-3743fb3030d2fc8c23f0dea11db0597e/dp/B0838KGSGF

Current-Limiting Resistor: https://www.amazon.com/Current-limiting-elements-2512-Resistor/dp/B0CQ3RY6LP

S8050 NPN Transistor: https://www.amazon.com/uxcell-100pcs-Transistor-Surface-SOT-23/dp/B07KPCBP24

JST 4-pin Connectors: https://www.amazon.com/Pairs-PH2-0mm-Female-Connector-Silicone/dp/B0DG92VWWK

NIST Cybersecurity Framework 2.0: https://www.nist.gov/cyberframework

OWASP IoT Project: https://owasp.org/www-project-internet-of-things/

OWASP. (2024). *IoT Security Guidance.* https://owasp.org/www-project-internet-of-things/

Microsoft. (2023). *The STRIDE Threat Model.* https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool\