I. Testing Device Introduction

- **Device Name:** Aqara Light Strip T1 and Sengled Bulb E11-N1EAW-2PK
- **Communication protocol:** Zigbee
- **Firmware version:** Latest
- **Complementary materials:** Wireshark traffic logs and firmware-version screenshot. Please use the following key in Wireshark to decrypt the traffic log: 0x0 0x1 0x2 0x3 0x4 0x5 0x6 0x7 0x8 0x9 0xa 0xb 0xc 0xd 0xe 0xf.

II. Security Issues

We first use our designed Zigbee security analysis tool to initiate a scanning procedure on the device. As a result, we found that the device supports the Zigbee Groups cluster (id 0x0004) on the endpoint 1.

Then we use our analysis tool to test the commands and attributes supported in these clusters. As a result, we identified the following security issues.

A. Denial of service with command "Get Group Membership"

- Then the attacker injects an GetGroupMembership command with a large GroupCount, e.g., 0xf0, and an empty GroupList.
- The device tries to transmit back a long list of GroupIDs, each of which is two bytes.
- The number of transmitted bytes overflows the transmission buffer of the target device. Eventually, the device will stop working and crash.
- Please check Line 106 - Line 117 (aqara.pcang) and Line 56 - Line 65 (sengled.pcapng) in the traffic log for more information.