- ## Vulnerability description

The Sengled Zigbee Smart Bulb devices contain a denial-of-service vulnerability, which allows a remote attacker to send malicious Zigbee messages to a vulnerable device and cause crashes.

- ## Affected product information

Name	Model	Firmware Version	Notes
Sengled Zigbee Smart Light Bulbs	E11-N1EAW	0x00000024	Amazon link

- ## CVE-ID

CVE-2022-47100

- ## Vulnerability type

Denial of Service

- ## Triggering vulnerabilities

The vulnerabilities are related to four commands, as shown below, which increase or decrease the brightness of the device at a certain *rate.* The rate field is of the uint8 type and is highlighted with color in the messages below.

Command	Normal message example -> exploit	Device initial state	Observations
`Move_up`(uint8)	0x01010003 -> 0x01010000	Brightness is set to the lowest (0)	Device crashed
`Move_down`(uint8)	0x01010102 -> 0x01010100	Brightness is set to the highest (254)	Device crashed
`Move_up_On Off`(uint8)	0x01050007 -> 0x01050000	Brightness is set to the lowest (0)	Device crashed

Move_down_OnOff(uint 8)	0x01050105 -> 0x01050100	Brightness is set to the highest (254)	Device crashed

To reproduce the crash, the device should be first at the “Device initial state”; after the exploit message is sent, the device crashes. For example, regarding the command Move_up(unit_8), the payload of a normal message example is 0x01010003, where the last byte 0x03 indicates the rate value. If the device brightness is currently the lowest, after the exploit message (whose rate value is 0x00) is sent, the device crashes. Specifically, we have the following two observations:

- If the exploit (i.e., 0x01010000) was sent once, the device flashes once, loses the connection, automatically changes to its factory status, and then rejoins the network after one second.
- If the exploit is sent multiple times within a period of time, the device loses the connection and cannot reconnect automatically until we ***manually pair*** it, allowing an attacker to conduct DoS attacks.

In other words, the Sengled Zigbee Smart Bulb cannot process the rate value 0x00 properly when the device is in certain states.

Attack vectors

By sending an exploit Zigbee message to the device

Discoverer

Xiaoyue Ma, Ph.D. student, George Mason University (xma9@gmu.edu)
Lannan(Lisa) Luo, Ph.D., Assistant Professor, George Mason University (lluo4@gmu.edu)
Qiang Zeng, Ph.D., Associate Professor, George Mason University (zeng@gmu.edu)