- **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_OnOff(uint8)	0x01050007 -> 0x01050000	Brightness is set to the lowest (0)	Device crashed
Move_down_OnOff(uint8)	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.

In another word, the Sengled Zigbee Smart Bulb cannot process the rate value 0x00 properly when the device is at certain states.

- **Attack vectors**

  By sending an exploit Zigbee message to the device