

- **Vulnerability description**

The Sengled Dimmer Switch device contains a denial-of-service vulnerability, which allows an attacker to send malicious Zigbee messages to the device and cause crashes.

- **Affected product information**

| Name | Model | Firmware Version | Notes |
|-----------------------|---------|------------------|-------------------------------|
| Sengled Dimmer Switch | E1E-G7F | v0.0.9 | Best Buy Link |

- **CVE-ID**

CVE-2023-29779

- **Vulnerability type**

Denial of Service

- **Triggering vulnerabilities**

The vulnerabilities are related to a command, `Set_short_poll_interval`, which can set the interval of the short poll, as shown in the table below. This command accepts one argument with the type `uint16`, which specifies the interval value.

| Command | Normal message example -> exploit | Observations |
|--------------------------------------|--|---|
| <code>Set_short_poll_interval</code> | <code>0x01030009 -> 0x01030000</code> | The device kept reporting state until the battery was drained |

After the exploit message (i.e., `0x01030000`) was sent, the device kept reporting its states with no interval and failed to respond to any normal messages. More importantly, in our experiments, the device drained its battery finally as a result of constantly reporting its status.

- **Attack vectors**

By sending an exploit Zigbee message to the device