- **Vulnerability description**

  Matter devices contain a denial-of-service vulnerability that allows an attacker to send malicious Matter messages to the devices, causing a denial-of-service problem.

- **Affected product information**

Name	Firmware Version	Notes
Govee LED Strip	v.3.00.42	Amazon Link

- **CVE-ID**

  CVE-2023-45956

- **Vulnerability type**

  Denial of Service

- **Triggering vulnerabilities**

  The vulnerabilities we discovered are associated with the `Move and MoveWithOnoff` commands (in the `Level Control` cluster), which are used to adjust the brightness of the lighting device. The `Move` and `MoveWithOnoff` commands operate by accepting two parameters: (1) the `MoveMode`, which is either 0 or 1, and (2) a `uint8 Rate` parameter. **The device crashes when the second parameter of the Move* command is 0.**

Testing Messages	Normal message example -> exploit	Initial Brightness	Observed Device Status
`Move(up, uint8)`	`Move(up, 1)` -> `Move(up, 0);`	`[1,254]`	Matter Lightstrip ***crashes***
`Move(down, uint8)`	`Move(down, 1)` -> `Move(down, 0);`	`[1, 254]`	Matter Lightstrip ***crashes***

`MoveWithOnoff(up, uint8)`	`MoveWithOnoff(up, 1) -> MoveWithOnoff(up, 0)`	`[1,254]`	Matter Lightstrip ***crashes***
`MoveWithOnoff(down, uint8)`	`MoveWithOnoff(down, 2) -> MoveWithOnoff(down, 0)`	`[1, 254]`	Matter Lightstrip ***crashes***

After configuring the device to its Initial Brightness state, we feed the `Move` or `MoveWithOnoff` testing messages to the device. We then observe a restart.

- The Govee device encountered a crash, characterized by an abrupt shutdown and a period of unresponsiveness.

- After executing the testing scripts, the `reboot count`(which belongs to the `general diagnostics` cluster) increased.

- **Attack vectors**

By sending an exploit Matter message to the device