- **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 |
  |---|---|---|
  | Nanoleaf Light strip | v.3.5.10 | [Amazon Link](Amazon Link) |

- **CVE-ID**

  CVE-2023-45955

- **Vulnerability type**

  Denial of Service

- **Triggering vulnerabilities**

  The bug is related to the `write binding attribute` command in the `Binding` cluster, which is used to establish a persistent relationship between an endpoint and one or more local or remote endpoints. This command accepts a list of parameters in the following two types: `List[node-id, endpoint-id, cluster-id]` or `List[group-id]`.

  | Command | Exploit | Observed Device Status |
  |---|---|---|
  | Write Attribute Binding | Write_Attribute_ Binding(0x654321, 1, 8) | Matter Lightstrip *crashes* |
  | Write Attribute Binding | Write_Attribute_Bind ingd(0) | Matter Lightstrip *crashes* |

Once this malformed command is sent, the Lightstrip crashed. 1) It flickered briefly and became unresponsive, resulting in a timeout exception. 2) The reboot count increased.

- **Attack vectors**

  By sending an exploit Matter message to the device