

- **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	<a href="#">Amazon Link</a>

- **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 Binding attribute	Binding( <span style="color: red;">0x654321</span> , <span style="color: red;">1</span> , 8)	Matter Lightstrip <b><i>crashes</i></b>
Write Binding attribute	Binding( <span style="color: red;">1</span> )	Matter Lightstrip <b><i>crashes</i></b>

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