

- **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
Govee LED Strip	v.3.00.42	Amazon Link
SwitchBot Hub2	v.1.0-0.8	Amazon Link
Phillips Hue hub	v.1.59.1959097030	Amazon Link
Yeelight smart lamp	v.1.12.69	Link

- **CVE-ID**

CVE-2023-42189

- **Vulnerability type**

Denial of Service

- **Triggering vulnerabilities**

The bug is related to the command `KeySetRemove (uint16)`, which is used to remove a given Group Key Set. This command requires one argument: `GroupKeySetID`, which has the data type `uint16` and its valid value is `[1, 255]`. To trigger the vulnerability, we provide an invalid value **0 or {}** (which means None parameter is provided).

Command	Normal message example -> exploit	Observations
<code>KeySetRemove (uint16)</code>	<code>KeySetRemove (1) -></code> <code>KeySetRemove (0);</code> <code>KeySetRemove (1) -></code>	The devices accept the crafted message.

	KeySetRemove ()	
--	------------------	--

Once this malformed command is executed, subsequent scripts may prompt the devices to respond with errors like "Invalid CASE parameter" or "No shared trusted root."

- **Attack vectors**

By sending an exploit Matter message to the device