

- **Vulnerability description**

The Fibaro Motion Sensor device contains a denial-of-service vulnerability, which allows an attacker to send malicious Z-Wave messages to the device and cause crashes.

- **Affected product information**

Name	Model	Firmware Version	Notes
Fibaro Motion Sensor	FGMS-001	v3.4	Amazon Link

- **CVE-ID**

CVE-2023-34597

- **Vulnerability type**

Denial of Service

- **Triggering vulnerabilities**

The bug is related to the “Clock” command class (0x81), which is used to sync the clock on the device with the controller system clock. To trigger the bug, we provided ***an invalid command id*** 0x01, which means that the corresponding command is not supported by (or does not exist in) the “Clock” command class.

Command	Exploit	Observations
An invalid command in the Clock cluster	0x 8101	Device crashed

After the exploit message was sent multiple times within a period of time (in our experiment, we send it 120 times in around 60 seconds), the device crashed.

- **Attack vectors**

By sending an exploit Z-Wave message to the device

- **Discoverer**

Xiaoyue Ma, Ph.D. student, George Mason University (xma9@gmu.edu)

Lannan(Lisa) Luo, Ph.D., Assistant Professor, George Mason University
(lluo4@gmu.edu)

Qiang Zeng, Ph.D., Associate Professor, George Mason University
(zeng@gmu.edu)