- **Vulnerability description**

  The Centralite Thermostat device contains a denial-of-service vulnerability, which allows an attacker to send malicious Zigbee messages to the device and cause crashes.

- **Affected product information**

Name	Model	Firmware Version	Notes
Centralite Thermostat	Pearl	0x04075010	official link

- **CVE-ID**

  CVE-2023-24678

- **Vulnerability type**

  Denial of Service

- **Triggering vulnerabilities**

  The vulnerabilities are related to a command, `Write_Battery_thres`, which can set a threshold for low battery alarms, as shown in the table below. This command accepts one argument with the type `uint8`.

Command	Normal message example -> exploit	Device initial state	Observations
Write_Battery_thres	0x02007d20 -> 0x02007d42	Heating mode is set to 32 degrees Celsius	Device crashed

  To reproduce the crash, the device should be first at the “Device initial state”---i.e., the device heating mode should be set to 32 degrees Celsius. As shown in the second column in the table, an example normal message is 0x02007d20, where the last two digits 0x20 represents the `unit8` data type. If we change 0x20 to 0x42, which represents the `CharString` data type, and set the device at the “Device initial state”, the exploit message 0x02007d42 causes the device to crash. Specifically, we have the following two observations:

- If the exploit (i.e., 0x02007d42) was sent once, the device lost the connection and reconnected automatically after around one second.
- If the exploit was sent multiple times within a period of time (in our experiment, we sent 50 commands in 100 seconds), the device lost the connection and could not reconnect automatically anymore, allowing an attacker to conduct DoS attacks. To reconnect the device, it required us to ***manually factory reset***, and ***manually pair*** the device.

Therefore, the Centralite Pearl Thermostat cannot process the `CharString` argument properly when the device is in certain states.

- ## Attack vectors

By sending an exploit Zigbee 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)