

- **Vulnerability description**

The Third Reality Smart Blind 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
Third Reality Smart Blind	3RSB015BZ	1.00.54	<a href="#">Shopping Link</a>

- **CVE-ID**

CVE-2023-29780

- **Vulnerability type**

Denial of Service

- **Triggering vulnerabilities**

The vulnerabilities are related to a command, Down\_close, which can extend the Smart Blind to the maximum length, as shown in the table below. This command does not accept any argument.

Command	Normal message example -> exploit	Observations
Down_close	0x0103 -> 0x010300	Device crashed

After the exploit message is sent, the device crashes. Specifically, we have the following two observations:

- If the exploit (i.e.,0x0103) 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 33 commands in 100 seconds), the device lost the connection and rejoined after around 30 seconds.

- **Attack vectors**

By sending an exploit ZigBee message to the device

- **Discoverer**

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

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

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