- ## Vulnerability description

  The Aeotec Wall Switch 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
Aeotec WallMote Switch	ZW130-A	v2.3	Amazon Link

- ## CVE-ID

  CVE-2023-34596

- ## Vulnerability type

  Denial of Service

- ## Triggering vulnerabilities

  The bug is related to the command `Firmware_Update_Request_Get (uint8, uint8)`, which is used to initiate a firmware update. This command requires two arguments: `ManufacturerID` and `FirmwareID`, both of which have the data type `uint8` and their valid values is [0,254]. To trigger the bug, we provide ***an invalid value*** 0xff.

Command	Normal message example -> exploit	Observations
`Firmware_Update_Request_Get`	0x7A038601 -> 0x7A03ff	Device crashed

  After the exploit message was sent, the device crashed and failed to respond to the following ping message.

- ## 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)