Boston Scientific
Advancing science for life™

ICS-ALERT-20-063-01
SweynTooth Vulnerabilities

The Boston Scientific team is dedicated to ensuring the safety and security of our products worldwide and has been closely monitoring the announcement regarding the vulnerabilities identified as “SweynTooth.” Many manufacturers offer hardware/software solutions – typically a System on Chip (SOC) – that implement a Bluetooth Low Energy (BLE) protocol. Some of these solutions have been reported to experience crashing or deadlock of the BLE hardware or may allow an attacker to bypass Bluetooth security features as communicated in the SweynTooth vulnerability disclosure.

Our product security team has assessed our medical systems that use BLE. At this time, we are not aware of any fielded Boston Scientific device that is impacted by this vulnerability, including our implanted devices. If this changes, we will provide an update.

For more detail, refer to:

- DHS: https://www.us-cert.gov/ics/alerts/ics-alert-20-063-01
- FDA: https://www.fda.gov/medical-devices/safety-communications/sweyntooth-cybersecurity-vulnerabilities-may-affect-certain-medical-devices-fda-safety-communication
- Asset Group: https://asset-group.github.io/disclosures/sweyntooth/

March 6, 2020