Safety Communication رسالة سلامة

SweynTooth Cybersecurity Vulnerabilities May Affect Certain Medical Devices

Device/ Product Description:	SweynTooth family
Brand:	Several brands
Affected product:	Medical devices from vendors who utilize BLE wireless communication technology. The affected medical devices may include pacemakers, blood glucose monitors, and others using affected BLE SDKs.
Manufacturer:	There are several system-on-a-chip (SoC) manufacturers that are affected by these vulnerabilities: ○ Texas Instruments ○ NXP ○ Cypress ○ Dialog Semiconductors ○ Microchip ○ STMicroelectronics ○ Telink Semiconductor
Problem:	The potential impacts of the SweynTooth vulnerabilities fall into three categories. An unauthorized user can wirelessly exploit these vulnerabilities to: • **Crash** the device. The device may stop communicating or stop working. • **Deadlock** the device. The device may freeze and stop working correctly. • **Bypass security** to access device functions normally available only to an authorized user.

Recommendation /Actions:	**Recommendations for Health Care Providers and Facility Staff:** • Work with device manufacturers to determine which medical devices in your facilities or in use by your patients could be affected by these vulnerabilities and develop risk mitigation plans. • Advise patients who use affected medical devices with steps they can take to reduce risk. • Remind patients who use medical devices to seek medical help right away if they think operation or function of their medical device changed unexpectedly. • Where possible, monitor medical devices for any signs of unusual behavior. For more information, Please click here. If you think you had a problem with your device or a device your patient uses, please do not hesitate to report the problem to SFDA through: NCMDR Vigilance system 19999 unified call center