FDA NEWS RELEASE

FDA Informs Patients, Providers and Manufacturers About Potential Cybersecurity Vulnerabilities in Certain Medical Devices with Bluetooth Low Energy

For Immediate Release:

March 03, 2020

Today, the U.S. Food and Drug Administration is informing patients, health care providers and manufacturers about a set of cybersecurity vulnerabilities, referred to as "SweynTooth," that – if exploited - may introduce risks for certain medical devices. SweynTooth affects the wireless communication technology known as Bluetooth Low Energy (BLE). BLE allows two devices to "pair" and exchange information to perform their intended functions while preserving battery life and can be found in medical devices as well as other devices, such as consumer wearables and Internet of Things (IoT) devices. These cybersecurity vulnerabilities may allow an unauthorized user to wirelessly crash the device, stop it from working, or access device functions normally only available to the authorized user.

To date, the FDA is not aware of any confirmed adverse events related to these vulnerabilities. However, software to exploit these vulnerabilities in certain situations is publicly available. Today, the FDA is providing additional information regarding the source of these vulnerabilities and recommendations for reducing or avoiding risks the vulnerabilities may pose to a variety of medical devices, such as pacemakers, glucose monitors, and ultrasound devices.

"Medical devices are becoming increasingly connected, and connected devices have inherent risks, which make them vulnerable to security breaches. These breaches potentially impact the safety and effectiveness of the device and, if not remedied, may lead to patient harm," said Suzanne Schwartz, M.D., MBA, deputy director of the Office of Strategic Partnerships and Technology Innovation in the FDA's Center for Devices and Radiological Health. **"The FDA recommends that medical device manufacturers stay alert for cybersecurity vulnerabilities and proactively address them by participating in coordinated disclosure of vulnerabilities as well as providing mitigation strategies. An essential part of the FDA's strategy is working with manufacturers, health care delivery organizations, security researchers, other government agencies and patients to address cybersecurity concerns that affect medical devices in order to keep patients safe."**

The FDA is currently aware of several microchip manufacturers that are affected by these vulnerabilities: Texas Instruments, NXP, Cypress, Dialog Semiconductors, Microchip, STMicroelectronics and Telink Semiconductor. Their microchips may be in a variety of medical devices, such as those that are implanted in or worn by a patient (such as pacemakers, stimulators, blood glucose monitors and insulin pumps) or larger devices that are in health care facilities (such as electrocardiograms, monitors and diagnostic devices like ultrasound devices).

Medical device manufacturers are already assessing which devices may be affected by SweynTooth and are identifying risk and remediation actions. In addition, several microchip manufacturers have already released patches. For more information about SweynTooth cybersecurity vulnerabilities – including a list of affected devices, see ICS-ALERT-20-063-01 SweynTooth Vulnerabilities, Department of Homeland Security Cybersecurity Infrastructure Security Advisory (https://www.us-cert.gov/ics/alerts/ics-alert-20-063-01).

The agency is asking medical device manufacturers to communicate to health care providers and patients which medical devices could be affected by SweynTooth and ways to reduce associated risk. Patients should talk to their health care providers to determine if their medical device could be affected and to seek help right away if they think their medical device is not working as expected.

The FDA takes reports of vulnerabilities in medical devices very seriously and today's safety communication includes recommendations to manufacturers for continued monitoring, reporting and remediation of medical device cybersecurity vulnerabilities. The FDA is recommending that manufacturers conduct a risk assessment, as described in the FDA's cybersecurity postmarket guidance (/media/95862/download), to evaluate the impact of these vulnerabilities on medical devices they manufacture and develop risk mitigation plans. Medical device manufacturers should work with the microchip manufacturers to identify available patches and other recommended mitigation methods, work with health care providers to determine any medical devices that could potentially be affected, and discuss ways to reduce associated risks.

The FDA will continue to assess new information concerning the SweynTooth vulnerabilities and will keep the public informed if significant new information becomes available.

Further, the FDA will continue its ongoing work with manufacturers and health care delivery organizations—as well as security researchers and other government agencies—to help develop and implement solutions to address cybersecurity issues throughout a device's total product lifecycle.

The FDA, an agency within the U.S. Department of Health and Human Services, protects the public health by assuring the safety, effectiveness, and security of human and veterinary drugs, vaccines and other biological products for human use, and medical devices. The agency also is

responsible for the safety and security of our nation's food supply, cosmetics, dietary supplements, products that give off electronic radiation, and for regulating tobacco products.

###

Inquiries

Media:

Emma Spaulding (mailto:emma.spaulding@fda.hhs.gov)

301-796-9423

Consumer:

888-INFO-FDA

Related Information

- SweynTooth Cybersecurity Vulnerabilities May Affect Certain Medical Devices: FDA Safety Communication (/medical-devices/safety-communications/sweyntooth-cybersecurity-vulnerabilities-may-affect-certain-medical-devices-fda-safety-communication)
- Department of Homeland Security Cybersecurity Infrastructure Security Advisory (https://www.us-cert.gov/ics/alerts/ics-alert-20-063-01)
- FDA Cybersecurity (/medical-devices/digital-health/cybersecurity)

More Press Announcements (/news-events/newsroom/press-announcements)