Health-ISAC Vulnerability Bulletin

Date: February 21, 2020 (**Updated March 4, 2020**)

TLP:WHITE

Event: UPDATE - SWEYNTOOTH Bluetooth flaws potentially impacting Medical Devices

Summary:
Health-ISAC published an initial Vulnerability Bulletin regarding SWEYNTOOTH on February 21, 2020 and is providing updated analysis and recommendations in this amended release.

SWEYNTOOTH captures a family of 12 vulnerabilities (more under non-disclosure) across different Bluetooth Low Energy (BLE) software development kits (SDKs) of seven major system-on-a-chip (SoC) vendors. The vulnerabilities expose flaws in specific BLE SoC implementations that allow an attacker within radio range to trigger deadlocks, crashes and buffer overflows or completely bypass security of Bluetooth enabled devices depending on the circumstances.

Analysis:
SWEYNTOOTH potentially affects IoT products in appliances such as smart-homes, wearables and environmental tracking or sensing. Researchers have also identified several medical and logistics products that could be affected.

SWEYNTOOTH vulnerabilities are found in the BLE SDKs sold by major SoC vendors, such as Texas Instruments, NXP, Cypress, Dialog Semiconductors, Microchip, STMicroelectronics and Telink Semiconductor. *By no means is this an exhaustive list of SoC vendors impacted by* SWEYNTOOTH.

Responsible disclosures accounted for almost all SoC vendors publicly releasing their respective patches. However, a substantial number of IoT products relying on the affected SoCs for BLE connectivity will still need to independently receive patches from their respective vendors.

Types of Vulnerabilities:

- **Crash:** Vulnerabilities in this category can remotely crash a device by triggering hard faults. This happens due to some incorrect code behavior or memory corruption, e.g., when a buffer overflow on BLE reception buffer occurs. When a device crash occurs, they usually restart. However, such a restart capability depends on whether a correct hard fault handling mechanism was implemented in the product that uses the vulnerable BLE SoC.
- **Deadlock:** Deadlocks are vulnerabilities that affect the availability of the BLE connection without causing a hard fault or memory corruption. Usually they occur due to some improper synchronization between user code and the SDK firmware distributed by the SoC vendor, leaving the user code being stuck at some point. Crashes originated from hard faults, if not properly handled, can become a deadlock if the device is not automatically restarted. In most cases, when a deadlock occurs, the user is required to manually power off and power on the device to re-establish proper BLE communication.
- **Security Bypass:** This vulnerability is the most critical one. This is because the vulnerability allows attackers in radio range to bypass the latest secure pairing mode of BLE. In summary, after the bypass is completed, an attacker in the radio range has arbitrary read or write access to a device's functions. These functions, in turn, are only meant to be accessed by authorized users.

Impact:
An attacker physically within radio range can use these attacks to perform denial of service and crash devices. However, a careful sequence of packets could be sent by the attacker to force the peripheral into writing certain contents to peripheral memory adjacent to the L2CAP reception buffer.

An attacker within radio range can use this attack to perform denial of service and crash the device. Given that a buffer overflow is being triggered depending on the packet, a remote execution scenario is a possibility. Furthermore, the SoCs affected by this vulnerability are known to be used in many smart home products, which increases the reachability and risk of a more serious exploit of this vulnerability.

Update (March 3, 2020) - **What We Know**：

- Health-ISAC is working closely with many Medical Device Manufacturers (MDMs) who welcome the hard work and diligence by the security researcher community in evaluating embedded systems. Their work makes the healthcare industry more resilient to cybersecurity attacks.
- The SWEYNTOOTH researchers developed viable exploits only for the devices they explicitly tested. They included a broad list of products that were not tested. Manufacturers of these devices and others leveraging SoCs should utilize their risk management process to assess the general risk level associated with these exploits and take commensurate actions.

- Manufacturers should consider BLE as a “zero-trust” component and leverage other controls and mitigations into their devices.
- Some system architectures segment functionality, so even if Bluetooth is compromised, other device functions may remain unimpacted.
- Vulnerability disclosure was pursued with the chip manufacturers, not with the downstream companies that leverage BLE chips and SoCs. As a result, testing and assessment for those impacted customers is ongoing.
- SWEYNTOOTH will not be the last of this kind of Bluetooth vulnerability; designing a robust and secure system architecture is better than chasing patches.
    - SWEYNTOOTH consists of multiple vulnerabilities, not all of which affect all devices.
        - Some vulnerabilities affect only a limited number of Bluetooth radios/ system-on-a-chip (SoC).
        - The vulnerabilities affect different devices differently.
    - Requires the attacker to be within radio range. Bluetooth range depends on several factors but can vary from 2 meters to greater than 1000 meters (For additional information: https://www.bluetooth.com/learn-about-bluetooth/bluetooth-technology/range/#estimator)
    - Bluetooth devices used in or near publicly accessible spaces are at higher risk than devices used in access-controlled areas.
    - Contact the device manufacturer to determine the design range of a device. Do NOT assume the effective communications range of a device is only a meter or two just because it uses Bluetooth.
    - Common Bluetooth devices used in hospitals that have been observed to exhibit ranges more than 100 m indoors include bar code scanners, audiometry systems and computers, to name a few.
    - The following list contains Bluetooth-enabled devices that may be found in the hospital environment, with many of them connected to the Hospital Information System (HIS). They may present to varying degrees, financial, data and patient safety risks. The list is not exhaustive.
        - Barcode scanners, e.g. for inventory and prevention of medication MIS-administration
        - Point of Sale (PoS) devices
        - Laboratory Point of Care (PoC) devices
        - Laptop, tablet and workstation computers
        - Computer peripherals, e.g keyboards, mice, printers
        - Computer display remote controls
        - Programmable implanted medical devices
        - Radiology devices and accessories
        - Radiological monitoring systems
        - Physiological monitoring devices
        - Long-term monitoring (Holter-like) devices

- Remote controls for therapeutic devices, e.g. electrosurgical units
- Audiometry systems
- Real-time location systems
- Smartphones and smartphone accessories, some incorporating medical devices
- Neonatal ICU audio and noise control systems
- Gait analysis systems
- Research instrumentation
- Environmental monitoring systems, e.g. pharmacy, research and pathology refrigerator/freezer temperature monitors

Health-ISAC released an initial Vulnerability Bulletin regarding SWEYNTOOTH on February 21, 2020.

Overall Recommendations
The FDA is urging stakeholders to determine whether any of their devices or systems are affected by the vulnerabilities, to perform cybersecurity risk assessments, and to undertake any appropriate risk management activities, to include short-term and long-term mitigations as well as communication with patients and any affected partners.

The FDA will provide updates on their next steps as they become available. Health-ISAC will share additional details and recommendations with Health-ISAC members as the information becomes available.

For more information regarding SWEYNTOOTH, please see the original Singapore University research report here.

Update March 4, 2020

- Health-ISAC maintains a web page that provides access to medical device manufacturers' product security websites. The URLs for each manufacturer listed will link to their product security site where you will find relevant security information.
- https://h-isac.org/mdm-security/

Update (March 3, 2020)

- The SWEYNTOOTH researchers at Singapore University developed viable exploits only for the devices they explicitly tested. They included a broad list of products that were not tested. Manufacturers of these devices and others leveraging SoCs should utilize their risk management process to assess the general risk level associated with these exploits and take commensurate actions.

- Health-ISAC urges members to familiarize themselves with NIST Special Publication 800-121 Guide to Bluetooth Security for best practices and security strategies regarding Bluetooth devices.

Recommendations for Health Delivery Organizations (HDO)

- Conduct an inventory to identify all Bluetooth-enabled devices. Maintain a complete inventory of all Bluetooth-enabled wireless devices and addresses (BD_ADDRs).
- Contact manufacturers to determine the characteristics of devices (SoC, version, range, patches and updates)
- Disable Bluetooth when not required.
- Pair devices only in controlled-access areas.
- Activate Bluetooth in access-controlled areas.
- Report unusual device behavior for investigation.
- Change the default settings when possible (device name, PIN code…).
- Install Anti-Virus software on Bluetooth-enabled hosts, where possible.
- Deploy Bluetooth software and firmware patches and upgrades.
- Reactive mitigation strategies
    - If an inventory of Bluetooth-enabled devices is not available, review the list of Bluetooth devices that may be found in the environment. Consider other uses similar to those listed where the facility may be using Bluetooth-enabled devices.
    - Prioritize the list of devices according to the facility's risk management plan and determine which devices should be investigated for mitigation and remediation.
    - Work with clinical staff to determine the presence and location of devices requiring mitigation and remediation.
    - Contact the manufacturers of any devices found to determine if the characteristics of the device warrant continued mitigation and remediation measures. These characteristics include:
        - Bluetooth radio/SoC manufacturer
        - Bluetooth version
        - Adherence to the NIST Bluetooth security guidance document during design and development of the device
        - Susceptibility to known Bluetooth vulnerabilities (Different versions of Bluetooth are susceptible to these vulnerabilities to different degrees… or not at all.)
            - Bluejacking
            - Bluebugging
            - BlueBorne
            - Key Negotiation of Bluetooth (KNOB)
            - SweynTooth
        - Designed effective communications distance more than 2 meters
        - A situation allowing, when considering the effective communications distance, detection and hacking in a location outside the normal location of use, e.g. a publicly accessible

area adjacent/near a patient room where an attacker can loiter unnoticed… a waiting room, cafeteria, or outside seating area.
        - Availability of updates and patches for known vulnerabilities
- Pre-emptive mitigation strategies
    - Develop a facility program to assess and prioritize risks from all wireless systems, including but not limited to Bluetooth.
    - Implement a pre-purchase/pre-implementation security review program.
    - Compare the device security to recommendations found in the NIST Bluetooth security guideline.
    - Ensure all Bluetooth profiles not necessary to the operation of the devices are disabled.
    - Ensure Bluetooth capabilities (as well as other wireless capabilities) are disabled when not required.
    - Enforce with corporate policies and Mobile Device Management (MDM) software, when able.
    - Instruct users of smartphones to turn off the Bluetooth function when it is not being used with an accessory or medical device requiring it.
    - Instruct users to pair devices only in controlled-access areas to limit access to Bluetooth signals during the paring process.
    - Instruct users to report erratic or unusual device behavior for investigation.

Recommendations for Mobile Device Management (MDM)

- MDMs should consider BLE as a “zero-trust” component and leverage other controls / mitigations into their devices.
- For IoT Manufacturers:
    - Change the default settings.
    - Set Bluetooth devices to the lowest necessary and sufficient power level.
    - Choose PIN codes that are sufficiently random, long and private.
    - Ensure that link keys are not based on unit keys (same keys to connect to every device).
    - Devices should use the appropriate security mode and level to support authentication and encryption after pairing.
    - Devices should not use the "Just Works" association model which does not require a PIN code to be paired (000000 by default).
    - Disable unneeded profiles (functionalities) and services.
    - Prompt the user to authorize all incoming Bluetooth connection requests.
    - Add application-level authentication and encryption (password, biometrics, smart card,…)

Request for Information (RFI)

Members willing to provide comments, make recommendations, share lessons learned, or best practices regarding this alert are encouraged to contact Health-ISAC directly at soc@h-isac.org.

References:

- SWEYNTOOTH

  https://asset-group.github.io/disclosures/SWEYNTOOTH/

- NIST Guide to Bluetooth Security

  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf
  Bluetooth LE devices impacted by SweynTooth vulnerabilities

  https://www.zdnet.com/article/unknown-number-of-bluetooth-le-devices-impacted-by-sweyntooth-vulnerabilities/

- Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients publication

  https://healthsectorcouncil.org/hhs-and-hscc-release-voluntary-cybersecurity-practices-for-the-health-industry/

- Health-ISAC medical device manufacturers' product security websites

https://h-isac.org/mdm-security/

A special thanks to Rickey Hampton from Partners Health and members of the Health-ISAC Medical Device Security Information Sharing Council (MDSISC) for their assistance in the creation of this document.

For questions or comments, please email us a soc@h-isac.org

Health-ISAC Threat Operations Center
100 Boeing Way Suite 1200, Titusville, FL 32780
(321) 593-1470
www.h-isac.org