Northwest Shelbyville Regional Hospital

Memo

To: Northwest Shelbyville Regional Hospital

From: Ralph Rodriguez

Date: March 28, 2025

Re: Vulnerability Memo

Device 1: Qardio Heart Health IOS Mobile Application

- Qardio simplifies heart health management by allowing you to record and store vital metrics, empowering you to make informed health decisions. It tracks blood pressure, irregular heartbeats, 12 body composition metrics (such as BMI, body fat %, muscle %, bone %, water %, etc.), weight, temperature, blood oxygen levels, and pulse rate. The Qardio app works seamlessly with award-winning devices: the QardioArm smart blood pressure monitor, QardioBase X smart body composition scale, QardioTemp forehead thermometer, and QardioSpO2 pulse oximeter.

- CVE-2025-23421: An attacker could obtain firmware files and reverse engineer their intended use leading to loss of confidentiality and integrity of the hardware devices enabled by the Qardio iOS and Android applications.

- Potential Solution:
    - When storing data in the cloud (e.g., S3 buckets, Azure blobs, Google Cloud Storage, etc.), use the provider's controls to disable public access.

- Feedback: CWE-552 highlights a vulnerability where files or directories may be accessible to unauthorized users, posing a security risk. However, the device can still be used safely if proper access controls, secure configurations, and network security measures are implemented. In cloud environments, ensuring sensitive data isn't publicly accessible, along with secure coding practices and regular system audits, can mitigate the risk, allowing the device to function securely despite this weakness. It is recommended to implement these security measures to ensure the device can still be used safely without exposing sensitive data.

- References:
    - https://www.cve.org/CVERecord?id=CVE-2025-23421
    - https://cwe.mitre.org/data/definitions/552.html
    - https://www.qardio.com/

Device 2: Contec Health CMS8000 Patient Monitor

- The Contec Health CMS8000 Patient Monitor is designed for clinical use across adult, pediatric, and neonatal patients, offering a range of customizable parameter configurations to meet various monitoring needs. Powered by 100-240V~, 50/60Hz, it features a 12.1" color TFT LCD that displays real-time data and waveforms, including eight channels of waveform and full monitoring parameters. An optional 48mm thermal recorder is available for enhanced functionality, and the monitor can connect to a central monitoring system via either wired or wireless networks. Capable of tracking essential parameters such as ECG, RESP, NIBP, SpO2, and dual-channel TEMP, this compact and portable device integrates the measurement module, display, and recorder in a single unit. Additionally, its replaceable internal battery allows for easy patient mobility, adding convenience to clinical settings.

- CVE-2025-0683: In its default configuration, Contec Health CMS8000 Patient Monitor transmits plain-text patient data to a hard-coded public IP address when a patient is hooked up to the monitor. This could lead to a leakage of confidential patient data to any device with that IP address or an attacker in a machine-in-the-middle scenario.

- Potential Solutions:
    - Identify and consult all relevant regulations for personal privacy. An organization may be required to comply with certain federal and state regulations, depending on its location, the type of business it conducts, and the nature of any private data it handles. Regulations may include Safe Harbor Privacy Framework [REF-340], Gramm-Leach Bliley Act (GLBA) [REF-341], Health Insurance Portability and Accountability Act (HIPAA) [REF-342], General Data Protection Regulation (GDPR) [REF-1047], California Consumer Privacy Act (CCPA) [REF-1048], and others.
    - Carefully evaluate how secure design may interfere with privacy, and vice versa. Security and privacy concerns often seem to compete with each other. From a security perspective, all important operations should be recorded so that any anomalous activity can later be identified. However, when private data is involved, this practice can in fact create risk. Although there are many ways in which private data can be handled unsafely, a common risk stems from misplaced trust.

> Programmers often trust the operating environment in which a program runs, and therefore believe that it is acceptable to store private information on the file system, in the registry, or in other locally-controlled resources. However, even if access to certain resources is restricted, this does not guarantee that the individuals who do have access can be trusted.

- Feedback: CWE-359 highlights a vulnerability where private personal information is exposed to unauthorized actors due to insufficient safeguards. While this presents a privacy risk, the product can still be used if proper mitigations are in place. Measures such as ensuring compliance with privacy regulations (e.g., GDPR, HIPAA) and using secure design practices, including encryption and access controls, can reduce the likelihood of unauthorized access. Additionally, careful handling of sensitive data and ensuring that logs do not store private information can help maintain the product's functionality while safeguarding privacy. Thus, the product can remain operational as long as these security practices are integrated.

- References:
  - https://www.cve.org/CVERecord?id=CVE-2025-0683
  - https://cwe.mitre.org/data/definitions/359.html
  - https://www.contecmed.com/productinfo/613024.html