Amenaza
TECHNOLOGIES LIMITED

Medical Device Manufacturer Case Study

Title: ***Critical vulnerability identified in embedded medical device***

Executive Summary

Several medical device companies are SecurITree® licensees and have received onsite training and advisory services from Amenaza. These companies produce devices for which safety and security are imperative. Their products include embedded devices (including pacemakers) and non-embedded devices (some of which interact with embedded devices).

These manufacturers have long had high standards of care in the design of their products. However, in light of the increasing connectivity of medical devices in a ever more hostile world, in 2023 the U.S. Food and Drug Administration (FDA) issued new regulations. The anticipation of these new requirements made improvements to existing security protocols necessary.

The head of product security at a prominent manufacturer applied Amenaza's technology and methodology to understand the cybersecurity risks associated with an upcoming product release. The project leader reported that the team discovered a serious, previously unidentified vulnerability that could, if exploited, cause serious health impacts on patients equipped with the device. Without Amenaza's guidance and technology, they indicated that it was very unlikely the fault would have been discovered before product release.

Identifying the issue before product release assured patient safety and saved the manufacturer millions of dollars in re-engineering and post deployment costs. It also avoided potentially expensive lawsuits from dissatisfied patients (and the pain and risks associated with revision surgeries).

Amenaza's Approach

Amenaza's methodology focuses on identifying the attack paths made possible by a system's architecture. This approach is more likely to identify flaws that would be otherwise overlooked. Amenaza's SecurITree technology makes it possible to evaluate thousands, or even millions, of potential attack strategies and identify those that are feasible for the adversaries the system may face. This in turn makes it possible for architects to incorporate architectural solutions into their systems that will remain resilient against present and future attacks.

Amenaza leverages the expertise possessed by its clients to create models that accurately reflect how systems will be attacked. Customer participation is essential to success. By combining client expertise with Amenaza's know-how and technology, risks can be identified and effective mitigation strategies defined. The customer is left with a clear understanding of any residual risk.

Amenaza
TECHNOLOGIES LIMITED

Why It Mattered

Successfully identifying a potential security flaw in an embedded device before it went to market benefited everyone. The medical device manufacturer avoided many costs (due to redevelopment, liabilities, legal costs) and a potential loss of sales and reputation. Patients avoided life threatening incidents and risky revision surgeries. Everyone (except, perhaps, the lawyers) were winners!