CENSUS
IT Security Works

CASE STUDY: MEDICAL APPLICATION

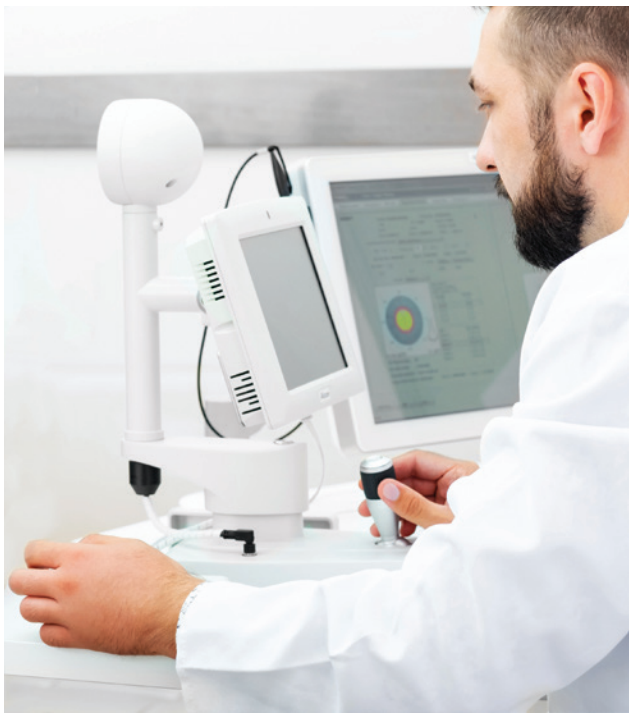
The present document describes activities performed and results obtained during Security Assessments conducted by CENSUS on a medical platform developed by an international vendor. Any information considered as identifying has been omitted intentionally in order to maintain confidentiality.

CENSUS was assigned the security assessment of a medical platform / solution, with multiple components, including a Bluetooth-enabled bioimpedance measurement device, an Android application that drives measurements and displays diagnostic information to clinicians, an application server that provides clinics with an API & Web Management interface, and a cloud service that collects anonymized patient measurements for further research.

The vendor's need was to prepare for and address early on any security issues that concerned the implementation of the platform. It was, however, equally important to be able to prove to third parties that security issues and risks were being proactively identified and managed.

Instead of running a standard security assessment of the platform prior to release, the organization chose to run a Secure Software Development Lifecycle (S-SDLC), introducing security processes within all stages of the development workflow. These processes included:

- Taking into consideration **security requirements** in the project requirements.
- Once suitable technologies were defined, the development team received relevant **security training**. Similarly, the Project Management team received training on S-SDLC best practices and how these could be applied to the established development workflow.
- **Design-level reviews** from a security standpoint highlighted architectural issues that required the team's attention.
- The codebase of each release was audited by means of both **code review** and functional security testing (Mobile and Web Application Testing). Testing also covered security aspects of the measurement device and its communications.
- Libraries were thoroughly examined for outdated, deprecated and **insecure third-party code**.
- Software bundles intended for installation on servers and mobile devices, were inspected prior to release for security and other **undesired artifacts**.
- The hosting environment of all services was thoroughly tested by means of **penetration testing** to identify environmental security issues.



- **Project security documentation** was developed and updated throughout all stages of the development lifecycle.

CENSUS supported the S-SDLC processes by providing the manpower and expertise required.

The project scope was to identify and evaluate platform vulnerabilities which could lead to potential cybersecurity risks for the vendor, for the users of the platform (i.e. physicians) but also for the patients. The risk measurements and recommendations made considered the sensitivity of the data processed (e.g. Electronic Protected Health Information) but also the criticality of the services offered by the platform.

The organization chose to run a Secure Software Development Lifecycle, introducing security processes within all stages of the development workflow.

KEY TAKEAWAYS

The S-SDLC assessments identified security defects of multiple types with the most prominent ones being information disclosure issues, business logic issues and authentication issues. Business logic issues are an important target in any security assessment, as these cannot be identified by automated processes and require a deep understanding of the intended product workflow.

Apart from the mere identification of security issues, the added value for the client was a long list of key takeaways.

SECURITY DOCUMENTATION

Security documentation is a key part of any Secure Software Development Lifecycle. Security efforts must be planned, security issues and decisions must be recorded, and security intelligence information must be disseminated to all parties involved. CENSUS delivered the following security documentation for this project: a Security Plan that recorded all security efforts of the project, an agent-based Threat Model that described the threats the platform was exposed to, a Security Architecture Document that justified the project's security controls, a Data Classification Document that grouped project data according to their sensitivity, and finally a Disposal Plan that explained the processes that must be carried out in order for the project data to remain secure in the case of a platform closedown, upgrade or migration action. Other sources of security information about the project were security design review deliverables, issue trackers and assessment reports.

AUDITED REUSABLE COMPONENTS

The client refactored the software in such a way, so that new features could build upon already audited components. This allowed assessments to focus on new code, thus minimizing the effort required for future assessments.

AVOIDANCE OF COMMON SOFTWARE VULNERABILITIES DUE TO SECURITY TRAINING

It has been observed that in the assessments of the two project releases that followed the development team's security training, no common vulnerabilities, such as SQL Injection, Cross-Site Scripting or Cross-Site Request Forgery issues, were identified. This accomplishment can only be credited to the development team's educational progress.

FDA GUIDELINES COMPLIANCE

Compliance with FDA pre-market and post-market cybersecurity guidelines was easy to achieve, as the required documentation and processes were already available due to the implementation of the S-SDLC.

ARCHITECTURAL ENHANCEMENTS

Design-level security reviews allowed for the early treatment of architectural defects (e.g. an insecure

certificate distribution mechanism). These are issues that commonly affect the core logic of a product and that may create project delays if they are identified during development (or later in the SDLC). CENSUS provided the necessary assessment and consulting to make sure that the client fully comprehended the risks involved in these design-level issues and proposed alternate schemes that were aligned with the project's security requirements.

CODE REVIEW ADVANTAGE

Code audits identified a number of issues that could not have been identified through "black box" testing methods. Such issues were:

- An Authentication issue related to a fixed (hardcoded) key used in session token creation, signing and verification
- A Race Condition which could force an illegitimate application update
- A Logging issue related to missing audit logs for clinician actions
- An Information Disclosure issue related to Personally Identifying Information being stored cleartext in the database

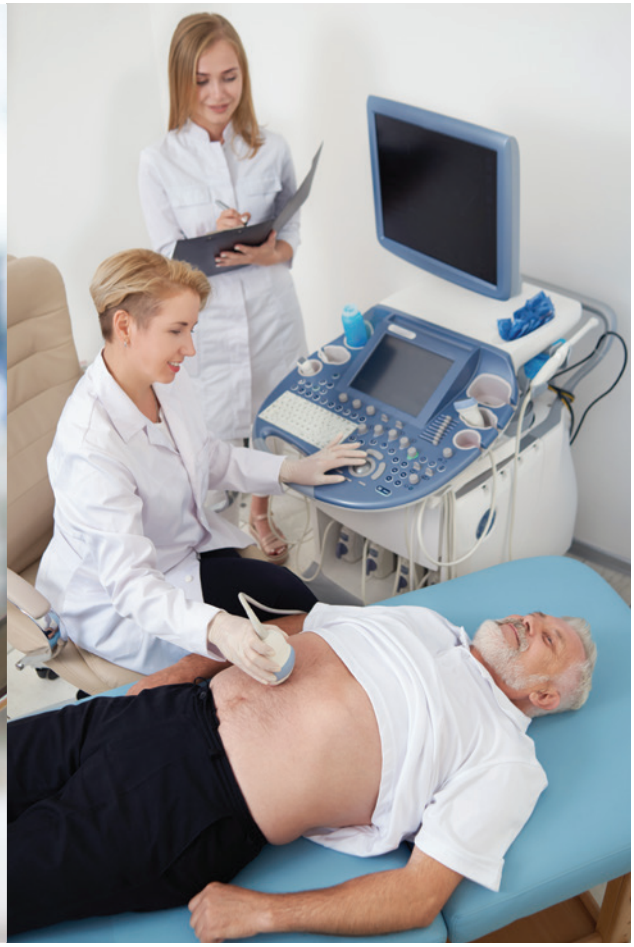
ACCURATE RISK ASSESSMENT

By utilizing functional security testing methods such as Web and Mobile Application Testing, code auditors were able to verify the actual risk involved in issues such as:

- Missing Access Controls allowing for the unauthorized publishing of software updates intended for measurement devices and mobile devices
- Insufficient Transmission Security protection, where the mobile application would deliver data to a man-in-the-middle attacker holding an invalid SSL certificate
- An Authentication issue that allowed the Administrator's password to be guessed during device registration

COMPREHENSIVE TESTING OF THIRD-PARTY TECHNOLOGIES

By performing focused testing on Bluetooth communications, a number of findings were revealed in a transport layer that was otherwise considered trusted by the measurement device & mobile app developers:



- An Authentication issue related to a fixed (hardcoded) key used to secure Bluetooth communications
- A Business Logic issue during signature verification that allowed unauthorized parties to issue arbitrary requests to the measurement device without knowledge of the secret communications key
- A Transmission Security issue that made all Bluetooth transmitted data vulnerable to eavesdropping and man-in-the-middle attacks

DISCOVERY OF RELEASE ENGINEERING ARTIFACTS

Through Bundle Inspection, release engineering artifacts were identified and fixed in the project's build process. Some of these artifacts were:

- A Binary Hardening issue where the application would expose sensitive information in backups.
- Dependency on Deprecated Third-Party Components, for which no security updates would be released.
- An Information Disclosure issue where software debugging logs were found to be enabled and would be stored in a publicly accessible path (i.e. accessible by any third-party application) on the mobile device filesystem.
- A Security Configuration finding where Android's security control for prohibiting unencrypted communications was not found to be enabled.

DEPLOYMENT ASSESSMENT

Through Penetration Testing and Host Configuration evaluation, the actual deployments of the platform were evaluated and issues such as the following were identified and corrected:

- A Host Hardening issue, where the RDBMS service was found to be accessible from the internal network of a clinic.
- A missing Access Control issue, allowing API Responses to be delivered to requests made by malicious JavaScript code hosted on any website on the world wide web.

About CENSUS

CENSUS is an internationally acclaimed IT Security service provider. Through its pioneering IT Security research, CENSUS delivers state-of-the-art services supporting organizations in multiple industries worldwide since 2008. The company's service portfolio includes Assessment and Advisory services, such as Security Testing, Code Auditing, Vulnerability Research, Digital Forensics, Training and Consulting. In 2017, CENSUS was enlisted as a Recommended Assessor for Medical Devices by Mayo Clinic, the non-profit academic medical center ranked as #1 in the Best Hospital Honor Roll by U.S. News & World Report.

CENSUS
IT Security Works

www.census-labs.com

USA
607 Boylston Street,
Suite 165L, Boston, MA 02116
T. 833-9CENSUS
E. usa@census-labs.com

UK
4th Floor, The Pinnacle,
Station Way, Crawley RH10 1JH
T. +44 1293 324 069
E. uk@census-labs.com

EUROPE
Stadiou 33, 10559,
Athens, Greece
T. +30 2102 208 989
E. eu@census-labs.com