Payatu

Payatu Casestudy

# A Leading Medtech Enterprise Assesses its Thick Client Application

Payatu Security Consulting Pvt. Ltd.

# Project Overview

This client of Payatu is a world leader in the field of medical technology aka medtech, and is driven to make healthcare better not just for its customers, but for the entire healthcare and medical industry. The company offers several innovative products and services under the umbrella of medical, surgical, neurotechnology, orthopedic, and spine to improve patient and hospital outcomes.

Security is now symbolic of reliability, which is why more and more organizations are undergoing a dramatic shift in the dynamics of how they integrate security in all their components. With the growing need for safe devices and services, companies are taking all the necessary measures to ensure that their offerings are not only compliant but also in alignment with the latest security practices to curb all malicious activities.

## The said client decided to opt-in for 2 of the most prominent services offered by Payatu

1. Thick Client Application Security
2. Security and Privacy Documentation

The Payatu security team performed real-time security assessments on the thick-client application of this client. These assessments were aimed at uncovering any security issues in the assessed thick-client application, explaining the impact and risks associated with the found issues, and providing the needed guidance in the prioritization and remediation steps.

As for the documentation, the client needed the Bandits to assist them in certain security and privacy documentation process. The company being a medtech company, it was critical for all its tools and devices to pass the security and quality checks before rolling them out in the market. These tools and devices are ultimately meant to work on a patient's body, making it extremely crucial for the assessor to fill in these documents so that they can further be assessed by an internal senior auditor. Once this process is carried out, only then can the products be launched on the market.

# The Scope

## Thick Client Application Security Assessment


## Security and Privacy Documentation

1. PSR Document that talks about mitigation practices to be implemented by developers and used for referencing to give a proper view to the auditor.
2. PSSA, similar to the PSR Document, is meant to talk about the mitigation practices.
3. SOM Document that is to be given to the users of the application and covers the measures to be implemented by the users for protection against malware, viruses, etc.
4. Test Case Document that talks about the test cases, expected results, observed anomalies/vulnerabilities.

# The Challenges

1. Application code was obfuscated which made decompiling, reading and comprehending difficult
2. Application taking inputs only from UI as user inputs were getting filtered from UI
3. License implementation was highly secure - licenses linked with devices and cannot be reused on another device, making it unable to bypass the application
4. Difficulty in extracting anything from cache logs because they were encrypted
5. Find cross references for each noted point in the document
6. Expansion of project – compliance check (Adding extra sections in the pentest report with proper POC)

# The Process

## Thick Client Application Assessment

1. Installing the application
2. Try to bypass the code obfuscation
3. Try to bypass the license – license check done
4. Manipulate the application configuration file to increase the license date
5. Supply payloads manually into the textboxes present in the application UI
6. Hijack application DLLs
7. Vulnerable library check
8. Provide malicious input files to the application to get RCE – remote code executes

# Documentation

## Thick Client Application Assessment

1. Conduct a detailed threat modelling exercise to identify all the potential threat vectors to the application
2. Preparing pentest report with an additional section for compliance testcases
3. Filling up the compliance-related document to provide a proper recommendation to the developers and clients' compliance audit team
4. Regular updating and fine-tuning of the documents based on compliance teams' inputs/recommendations.

# Recommendations

1. Application should be updated with the latest version of dependencies.
2. Application should not be allowed to get installed in shared directory/path.
3. The application binaries should be obfuscated and should not take any runtime inputs from user console.
4. The permission to binaries should be appropriate so that only authorized system users have access.
5. Proper Code review of application before releasing.
6. Anti-dynamic instrumentation techniques should be implemented in application.
7. The log files should not contain sensitive user information and license information.
8. The treatment plan directory should only be accessible to system user using the application.

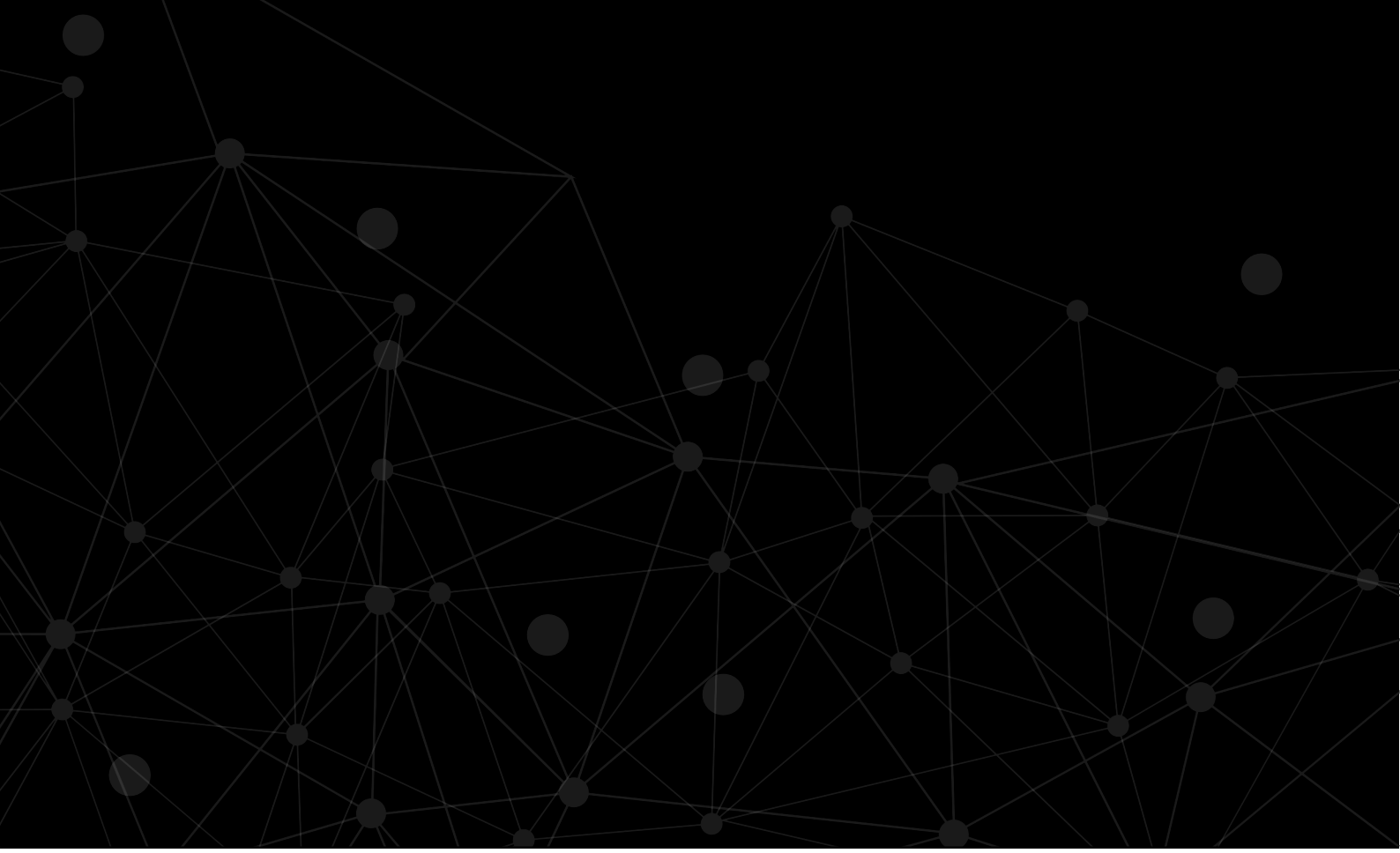
Payatu

# About Payatu

Payatu is a Research-powered cybersecurity services and training company specialized in IoT, Embedded Web, Mobile, Cloud, & Infrastructure security assessments with a proven track record of securing software, hardware and infrastructure for customers across 20+ countries.

Our deep technical security training and state-of-the-art research methodologies and tools ensure the security of our client's assets.

At Payatu, we believe in following one's passion, and with that thought, we have created a world-class team of researchers and executors who are willing to go above and beyond to provide best-in-class security services. We are a passionate bunch of folks working on the latest and cutting-edge security technology.



Payatu

**Payatu Security Consulting Pvt. Ltd.**

www.payatu.com
info@payatu.com
+91 20 41207726