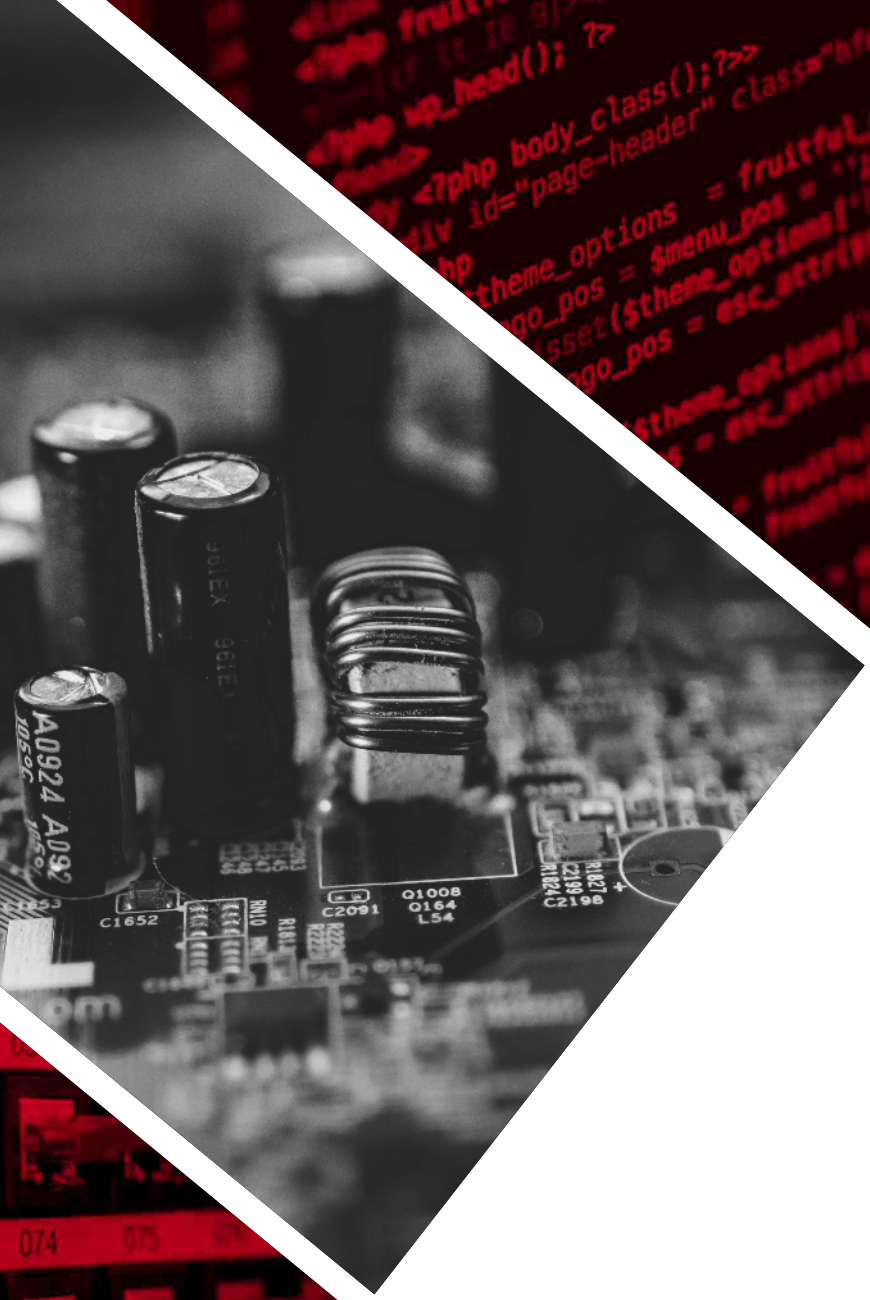

Payatu

Infrastructure Assessment of an IoT Ecosystem

Payatu Casestudy

Problem

Our client is a German company that offers IoT-based solutions for smart buildings to turn any commercial facility into a smart building. Their services also have a range of automation in the IoT space for smart buildings.

To make their solutions robust and foolproof from intrusions, they wanted to test the whole ecosystem's security aspects. This included the hardware, cloud, web interface, and code review. They reached out to Payatu to test the IoT ecosystem of their products and services.

Solution

The Payatu research team did a comprehensive assessment and found multiple vulnerabilities that impacted their IoT offerings' security. The evaluation was aimed at:

Hardware

- We were able to boot the device from the SD card successfully. This can help intruders to control the device in whichever way they wanted.
- The solution used a radio protocol, which was based on IEEE 802.15.4, for communication. We mapped and performed security assessment on the radio network and could decrypt the communication and view the sensitive information.
- We were able to extract the encryption key used for securing the radio communication from the hardware.
- We found that the encryption key was common across all the devices in the ecosystem, and compromising one device could lead to sensitive data leakage in the radio network as well as compromise all other devices and gateways.

Web interface

- The access control mechanism in the application was not implemented properly. It allowed us to collect all the connected users' information, including some of the personal data.
- We were able to delete and modify the credentials of other users.

Code review

- We found hardcoded credentials in multiple places in the source code like MQTT credentials and license keys.

Benefits

With our assessment, the client was able to protect user-sensitive information. Any data leakage with personal critical details can result in frauds and financial losses to the end-users and the client. The testing identified the loopholes in the infrastructure. We could also help the client to protect their IoT system's intellectual property by identifying the vulnerable parameters.

The project took nearly 4 weeks for completion.

About Payatu

Payatu is a Research Focused, CERT-In impaneled Cybersecurity Consulting company specializing in security assessments of IoT product ecosystem, Web application, Cloud, & Network with a proven track record of securing applications 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 Security Consulting Pvt. Ltd.

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