Payatu

Security Assessment of an IoT-Based Fleet Management System

Payatu Casestudy

Problem

Our Client, one of Asia's top telecom service providers, offers GSM-based monitoring devices for the fleet management system. These devices are connected to the servers over the cloud. The device monitors (but does not change) vehicle parameters like tire pressure, heat levels in the engine, vehicle location, fuel consumption, distance covered, etc.

To evaluate the security of the devices, the company reached out to the research team at Payatu. The goals of the penetration testing were to identify:

- Loopholes that allow intellectual property theft, which a perpetrator can use to sneak away with the device's firmware design.
- What kind of attacks are possible that can compromise the device communication? If tampered with by an unauthorized user, the device might lose sending (right) data to the cloud server.

Solution

Following are the ways we used for testing, issues that we identified, and the impact it could have on the fleet management system:

1. We could access the root shell through USB interface by running exploits like Kernel vulnerability leading to:
   a. Admin access to the attacker that gives complete control on the system,
   b. Open channels for remote attacks.

2. After getting root access, we were able to install malicious application inside the device that allowed us to:
   a. Replicate device functionality by reverse-engineering the system using the exposed binaries,
   b. Read files, credentials, and keys,
   c. Implant malicious code in the firmware.

Having mitigated these risks in the system, the telecom giant took their fleet monitoring device's security to the maximum.

Results

A data-backed fleet management system proves to be highly effective in the case of commercial vehicles. And security threats can cause issues.

IP theft can result in a massive loss to a manufacturer. With our assessment, the company could identify all the possible security gaps leading to design theft and saved themselves from financial losses.

Spoofing a vehicle's parameters like GPS coordinates can lead to false tracking and end up with manipulated pricing, location, and vehicle availability. The vehicles in such situations can also cause financial fraud.

The project was on a very tight schedule, and we could complete the assessment in 2 weeks.

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