Payatu

IoT Security Assessment of a Medical Device

Payatu Casestudy

Problem

One of the world's leading medical equipment manufacturers wanted to assess the security of one of their devices. The device called a **medical stapler** is used for stitching the wounds and cut during surgical processes in hospitals.

The objective of the assessment was to compromise the IoT system connecting the devices from various dimensions. This would help them in identifying the security vulnerabilities, which could impact in these ways:

- Malfunctioning of medical devices can lead to life-threatening issues.
- Patients' data and medical analysis are sensitive personal information that can cause problems when leaked.
- In the case of ransomware, data threats can escalate to severe issues that can cause financial losses to the hospitals.
- Another critical aspect of IoT security is to protect the intellectual property of the firmware designs.

The client reached out to Payatu for the assessment.

Solution

A medical stapler connects with a controller using WiFi.

The security assessment included testing of communication between the stapler and the controller, identifying entry points to hack the design of the firmware, and any other possible intrusion route into the system.

We performed the following vulnerability assessments on the IoT system:

Physical access of the device

We could identify the medical stapler's address and sent a continuous de-auth request to the Access Point leading to disconnection of the communication between the two. This caused a denial-of-service (DOS) attack and jammed the communication.

This kind of attack is possible even when the attacker is not in the same Wi-Fi network.

Impact

Any disruption in a medical device's availability during surgeries can suspend the procedure and cause life-threatening situations.

Proximity access of device

We could perform a MITM (man in the middle) attack by placing ourselves between the device and the controller. Now the communication happening between the medical staplers and the controller was passing through us.

Once the imposter gets into the devices' network, they can take over and control the communication completely.

Impact:

An attacker can capture the login credentials from the web panel entered by the victim on other machines. They can then manipulate the communication between the devices. This can lead to the loss of lives, data, or finances.

Broken authentication and session management

We could send unauthenticated requests without being logged in to the devices. Remote access of a device web interface can make this attack possible through any open port accessible via the network.

Impact

The attacker can use this glitch and become an admin or add new users and change the settings. This could allow the attacker to cause a Denial of Service, hack credentials, and control the device, making the device dysfunctional.

Results

Medical devices demand 100% availability and should function correctly round the clock. After our assessments, the company could avoid all the issues that might have culminated in losses of Millions and hazardous data breaches.

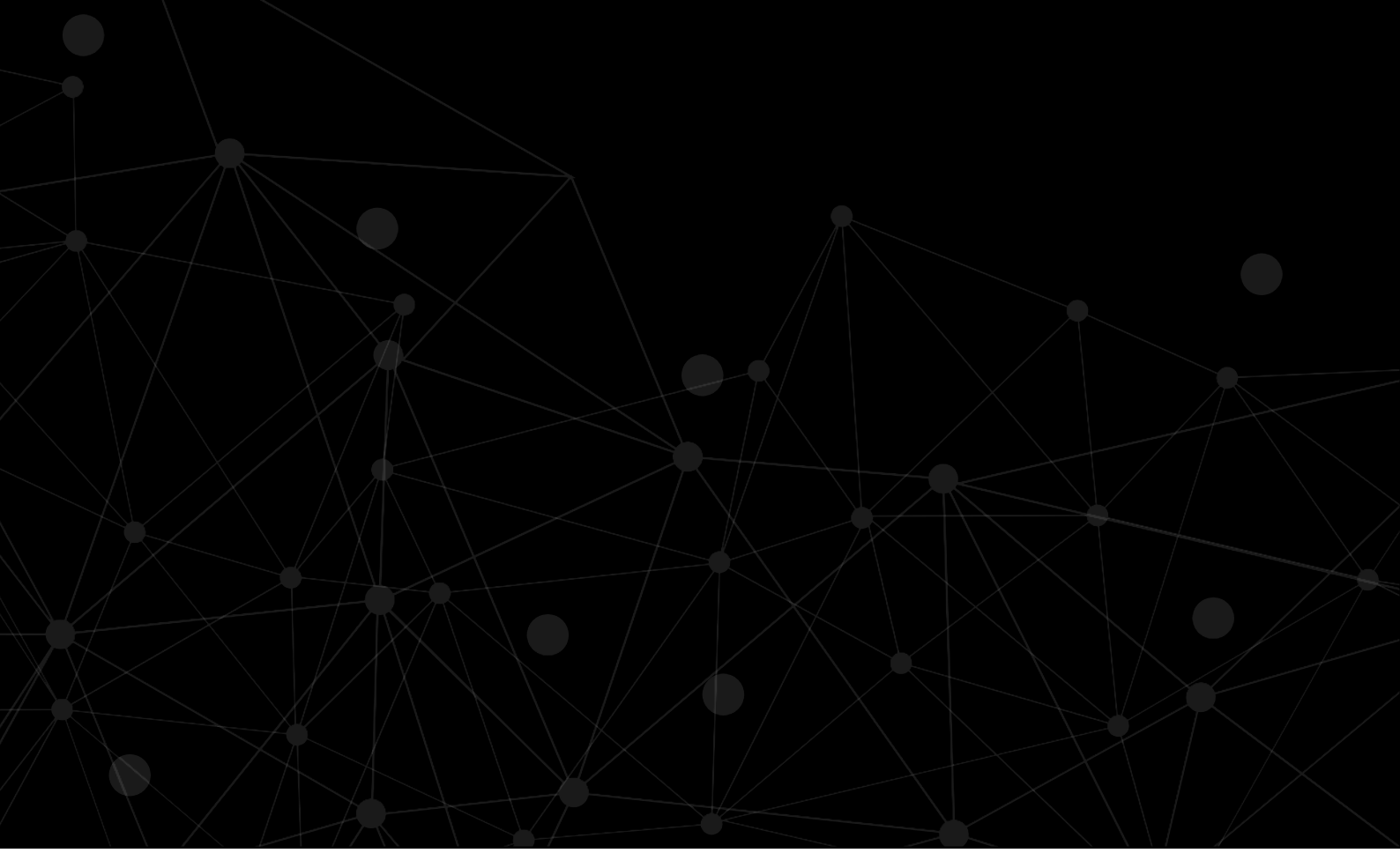
The project took 3 weeks for completion.

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