Payatu

Security Assessment of Critical Healthcare Equipment

Payatu Casestudy

Problem

One of the largest manufacturers of medical devices wanted to assess their medical equipment's security. So, they contacted the team at Payatu for a comprehensive security assessment.

None of the medical devices like the MRI and X-ray machines should malfunction. Even a minor glitch in these machines can cause life-threatening issues. A hospital's medical devices are required to have round-the-clock availability, as well. Additionally, patient data integrity and confidentiality are essential, too.

The client wanted us to assess the devices on two parameters:

1. The device should be available round the clock and should not malfunction.
2. No one should duplicate the firmware's design by stealing the intellectual property of the manufacturer
3. Patient data must not be accessible to an unauthenticated user.

Solution

For a comprehensive test, we tested the devices in the following ways:

Area Impacted	IP, Availability	Availability, Integrity	Confidentiality
Assessment Outcome	Firmware recovery by eavesdropping device firmware upgrade (DFU)	IR command injection and device information extraction	End-to-end encryption is missing on network interfaces
Vulnerability Description	We could eavesdrop on the device firmware upgrade and extract the firmware from the communication.	An attacker in the proximity can inject commands over the Infrared interface as there's no user authentication.	Network communication to and from the equipment is not encrypted.
Exploitability Rationale	The attacker could capture the network traffic, identify the firmware headers and length, and then use them to recreate the firmware.	The attacker in proximity can intrude at any time.	The attacker on the same network can eavesdrop on the information being exchanged.
Impact Rationale	The attacker can access the file system, business logic, intellectual properties, and credentials from the firmware. This can lead to further attacks, including firmware modification (backdooring), privileged access to the device, etc.	The intruder can brick the device, modify calibration data, change the Wi-Fi network, switch on or off some of the device features or affect the device availability.	Leakage of information such as firmware design, X-ray images, business logics, intellectual properties, and device credentials.

Benefits

Tampering medical equipment to steal intellectual property is not uncommon. This causes financial loss to the manufacturers every year. However, with medical devices, the biggest threat is human lives. And data leakages, device malfunction, and outages can cause harm to life and patient data theft, to say the least. The worst could lead to life-threatening problems.

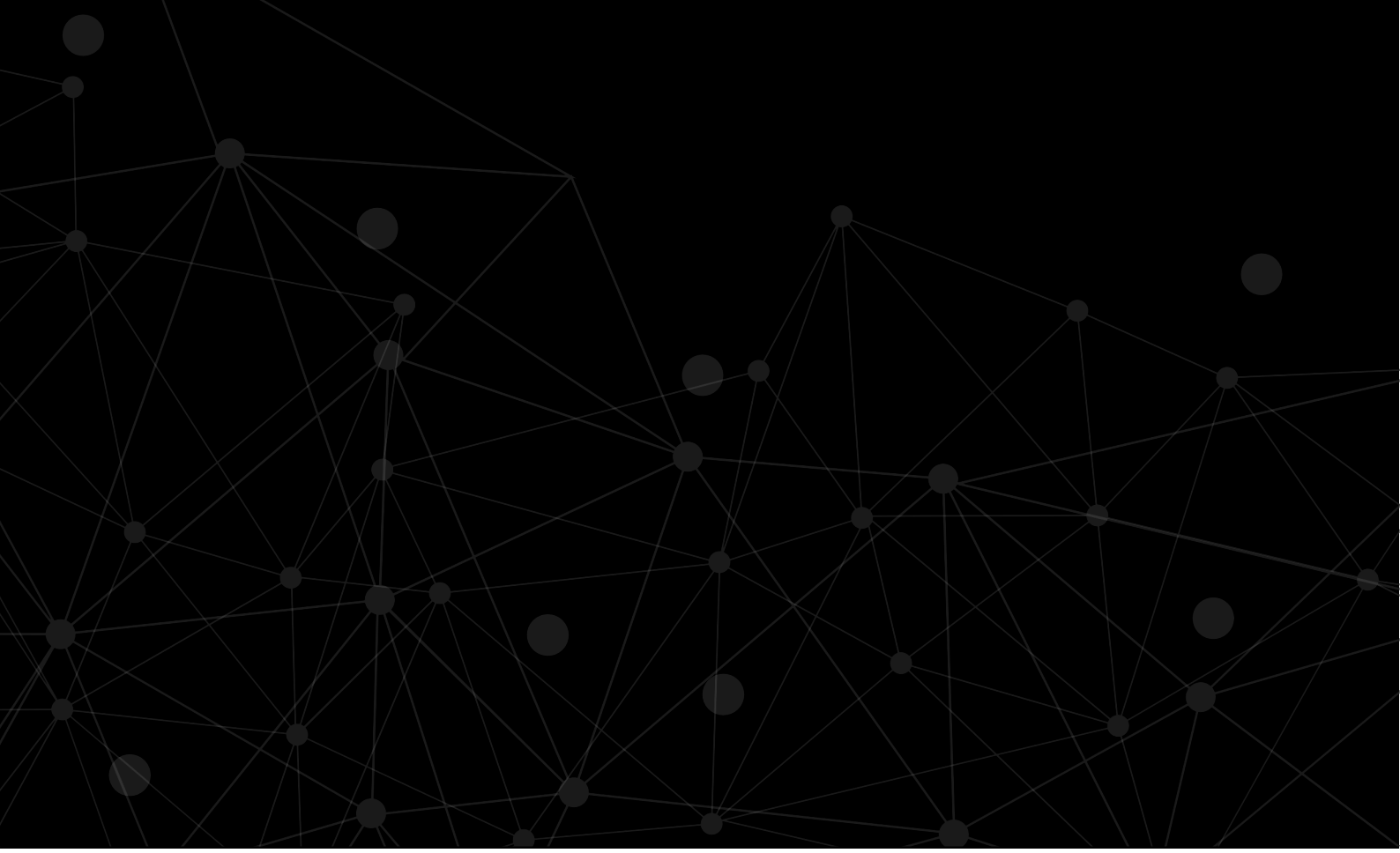
Our rigorous security assessments helped our client to mitigate the shortcomings in the equipment from the security front. Their outage windows also shrunk to a negligible level that is manageable for the operators.

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