

HEALTHCARE CASE STUDY

Industry
Healthcare

Client Background

One of the largest healthcare organizations in the world, leveraging data-driven technologies to address substantial unmet clinical needs. The goal of using deep learning on radiology imaging is to improve diagnosis for critical specialized clinical areas. Their software analyses CT imaging to provide a quick and accurate diagnostic report on lung issues.

Environment

- Focus on bridging Diagnostics over 1 billion respiratory Patients Globally.
- Established in 2016.
- Main product is LungIQ.

Business Challenges

- Due to the large burden of chronic obstructive pulmonary disease, it is difficult to track each patient's progress.
- Technology is crucial in ensuring that patients receive the best possible care. As a result, it must be technologically updated on a regular basis.
- Develop an appropriate compromise between security best practices and equipment operating difficulties.

Solution

Kratikal's expertise in healthcare management systems and detection of technical and logical vulnerabilities that could undermine the operation of their AI software-enabled medical equipment connected to the network was sought by the healthcare provider. They also required concrete actions to mitigate the hazards that could arise because of those weaknesses being exploited.

Approach

- The tests were carried out in a live environment, during times of no traffic on the machine.
- The test was conducted as a gray box exercise.
- Various hacks were attempted to test the medical devices, the consoles, and the network connection.
- The tests were conducted under the best practices available in the industry, using the experience of Kratikal in Medical Device Security Testing and IoT device testing practices.



Major Findings

- By simply including the username argument in the password reset request, an attacker can gain control of any user account. This could pose a severe security risk to the platform's users.
- Application is vulnerable to Host Header Injection where Attacker can redirect victim to any phishing or untrusted site by using the header of any malicious website.
- One of the findings was Weak Lockout Mechanism, which states that if the application has a strong lockout mechanism, it may be subject to brute force attacks.
- Passwords that are guessable and easy to crack using brute force, dictionary, or rainbow table attacks are made possible by weak password policies.
- Attackers can produce the reset link several times by replaying the password reset request. If there are no rate constraints, the attacker may spam the user's email with password reset links.
- If the session has already been hijacked, it will stay active even after the password has been reset.
- Using an outdated version of TLS for data encryption in transit can jeopardize such sensitive data. Because the data it encrypts can be decrypted or changed.

Risks

- By simply including the username argument in the password reset request, an attacker can gain control of any user account. This could pose a severe security risk to the platform's users.
- An attacker can send a victim to any phishing or untrustworthy website using the header of any malicious website.
- An attacker with remote access to the server can exfiltrate sensitive data, undermine the integrity of application data, or cause the program to stop working.
- After a successful brute force attack, a malicious user may gain access to confidential information, administrative panels, and the ability to launch additional attacks.
- Weak password policies make passwords easier to guess and crack using brute force, dictionary, or rainbow table attacks.
- If rate limits are not specified, the attacker may send password reset links to the user's email address.
- Using the vulnerabilities, an attacker could steal confidential patient records from the systems.



Impact

- An attacker could exploit these vulnerabilities that could lead to life-threatening conditions for patients.
- Attacks on the critical instruments, particularly the ones dealing with nuclear medicine and radiology could lead to an equipment malfunction in the best case and unchecked radiation leakage in the hospital as the worst-case scenario.
- Being a publicly traded healthcare firm, the hospital could face huge lawsuits, sanctions, and loss of share price along with a PR fiasco.
- Weak BLE and WiProtocols were a huge risk to confidentiality and availability.




Recommendations

- A strong password policy that only accepts passwords with at least 8 characters and at least three of the four-character sets (capital letter, small number, number, and special character).
- A detailed report was provided on the vulnerabilities along with their impact and recommendation techniques
- When a user signs out of an application, it is suggested that the session expires on the server.
- Backend verification/input validation should be used to ensure rate limits on critical functions such as: - Putting together legal documentation, creating obstacles, making any adjustments on the client's end, and Notification mechanisms such as email or one-time passwords.
- When a user updates their password in an application, it is advised that the session expires on the server side, or that the user be given the choice to terminate logged in sessions.
- It is recommended to implement Anti-CSRF tokens and same site flag in a cookie should be set.
- It is recommended to Include HSTS header in the response.


Kratikal Privacy commitment

Kratikal is dedicated to safeguarding your company from advanced threats, such as data leakage. For this reason, we do not reveal the names of our case study participants.

 +91 9289192210

 sales@kratikal.com

 www.kratikal.com

 A-130, 2nd Floor, Sector 63, Noida, Uttar Pradesh, India-201307