KRATIKAL
SECURE FOR SURE

SAAS CASE STUDY

Industry

SAAS

Client Background

The company is a SaaS based solution provider and has over 15000+ businesses across 65+ countries. They are the leading cloud communication provider in emerging markets in less than 7 years. We've matured to becoming a globally recognized named with over 600 employees

Business Challenges

- Assess vulnerabilities present in the application of the company.
- Protecting the user data from being misused and made public.
- Safeguarding the application from being abused to distribute malware.

Environment

- 15000+ Business Users
- Operates around 65 countries
- Trusted by some of the biggest IT firms of the world

Solution

The company approached the security testing department of Kratikal to identify the technical as well as the logical vulnerabilities that may be present in their cloud application which they provide as a SaaS to their customers. To seek recommendations for mitigating the potential risks that may arise on exploiting those vulnerabilities.

Approach

- The test has been carried out in a dummy environment.
- The test was conducted as a black box exercise.
- Various hacks were attempted to test their web application.
- The tests were conducted in accordance with the best practices available in the industry, such as Open Web Application Security Project (OWASP).

Major Findings

- It was discovered that the parameters corresponding to the billed amount of subscription can be modified such that, it could be bought for FREE.
- Confidential information about all their customers could be drawn out of their servers
- The SSL mechanism to encrypt confidential information like usernames and passwords was incorrectly configured.
- Using the web app, the email id and SMS of the customers could be bombarded with emails/SMS.
- Account of the admin user could be hijacked by the attacker.
- OTP verification over mail or SMS was susceptible to brute force attacks.

Risks

- Since the parameters corresponding to the billing amount can be tampered with, the attackers can buy subscription of their product for FREE.
- Using the OTP verification mechanism, the attackers could flood the SMS/- Mail box of the users of their service
- Because of insufficient protection at the transport layer, attackers can sniff the data (going to the server from the Mobile application) and modify it.
- An attacker could target their clients with spear-phishing emails and SMShing using the data leaked from their servers.
- Usernames and Passwords of the users were leaked from their application.

Impact

- Modifying the pricing parameter, one could buy their subscription for FREE, resulting in losses of over ₹10 Crores.
- Leaking of sensitive client information from their application about their clients and users can make them liable for huge fines under various compliances and local cyber laws of the countries their work in.
- Hijacking of the admin accounts of their application could lead to complete loss of service.
- Using the application's functionality, the attacker could redirect the users to malicious sites and install malwares like ransomwares into their systems and networks.
- The company could face huge financial losses, potential lawsuits and defilement of their brand image.

Recommendations

- To deal with the issue of parameter tampering, we suggested the organization that parameters should be verified at the server and the response of the server should be matched with the request sent by the application.
- We suggested critical changes in the application's architecture and authentication mechanism.
- We advised the organization on advanced controls and cryptographic techniques (like obfuscation techniques) for database security and server design.
- We suggested them to modify their application flows to prevent data loss and account takeovers.
- Detailed documentation of the vulnerabilities discovered in the application was provided, explaining the problem, its cause and remediation.

Free Consultation

Would you like to determine your company's risk exposure?

Drop us an email and we'll respond as soon as possible.

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.

"We sought help from guys at Kratikal when it dawned upon our team that getting an external perspective into how we are performing would be a great thing! Talking to their team gave us good insights and confidence into their capabilities. In the penetration testing results that they have uncovered, we came across few gaps which our teams couldn't have identified or spotted. We are extremely satisfied with our decision to work with them."

-Director (Mobile & Internet), SaaS Provider

+91 9289192210
sales@kratikal.com
www.kratikal.com
A-130, 2nd Floor, Sector 63, Noida,
Uttar Pradesh, India-201307