DETEACT

SECURITY ASSESSMENT REPORT

SIA JITBIT BALTIC

Deteact, 2021

CONTENTS

1 GENERAL INFORMATION

This report contains information about the results of the security audit of SIA Jitbit Baltic (hereafter referred to as "Customer"), conducted by Deteact in the period from 12/14/2020 to 01/18/2021.

1.1 Introduction

The purpose of the testing is:

- Security assessment of the Customer's web applications, including attempts to gain access to the critical assets and confidential data,
- Development of the short-term and long-term technical and organizational recommendations based on the findings and industry best practices,
- Evaluation of applied bug fixes and security improvements, control checks of the findings.

Tasks solved during the testing:

- Security audit of the infrastructure, development process, and the cryptographic mechanisms,
- Reconnaissance of the web platform endpoints and environment,
- Known 3rd party software vulnerabilities identification and web application file system enumeration,
- Automated vulnerability scanning of the identified web applications, manual verification of the results,
- Search for incorrectly deployed development/testing/debugging versions of software, administrative interfaces,
- Checking for default credentials, credentials brute force,
- Rechecking of the fixed weaknesses and vulnerabilities.

1.2 Scope of Work

The testing scope included the cloud (SaaS) version of the Jitbit product. Deteact deployed several workspaces for testing purposes.

1.3 Threat Model

The assessment simulates the actions of an external intruder, described by the following characteristics:

- Has no physical access to devices and the Customer's network, connects to them through the Internet,
- Has knowledge and experience of exploiting well-known vulnerabilities of web applications and network services,
- Uses the combination of wide-spread open-source and commercial tools for searching and exploiting the vulnerabilities,
- Aims to access or damage the Customer's sensitive information, client data,
- Has limited computing resources and time,
- Acts alone or in a small group,
- Has no prior knowledge about the company's network and doesn't have special privileges.

Therefore, the most critical threat for the Customer's product is theft, malicious manipulation, or damage of the client data.

1.4 Weakness Scoring

The findings in this report are scored by an expert evaluation, an impact of each vulnerability is calculated based on its ease of exploitation and severity (for the considered threats).

2 SUMMARY

During the testing of the Customer's web applications several high impact issues have been identified. All the high and medium risk vulnerabilities have been fixed within a month after report.

The identified vulnerabilities could pose a risk to the Customer's product, but after the appropriate mitigations have been applied, the overall security level of the Customer's infrastructure and software can be described as **high**.

2.1 Findings Status

The table below contains information regarding the current (as of 02/01/2021) status of the identified issues. Some of them require more attention and should be fixed as soon as possible, some of them do not pose an immediate practical risk.

Table 1. Status of the identified issues

Finding	Risk Level	Status
Cross-Site Scripting in ticket comment rendering (XSS)	**High**	Fixed
Cross-Site Scripting in user info (Stored XSS)	**High**	Fixed
OAuth Hijacking	**High**	Fixed
User Data Leakage and Privilege Escalation (IDOR)	**High**	Fixed
Comment Author Spoofing (IDOR)	**Medium**	Fixed
Ideas Tag and Status Spoofing (IDOR)	**Medium**	Fixed
Comment Hijacking (Improper Access Control)	**Medium**	Fixed
Ticket Information Leakage (IDOR)	**Medium**	Fixed

Finding	Risk Level	Status
Ticket Author Spoofing (IDOR)	Medium	Fixed
Broken Multi-factor Authentication	Medium	Fixed
Server-Side Request Forgery in the account view (SSRF)	Medium	Fixed
User Enumeration	Low	Fixed
Cross-origin Resource Sharing Misconfiguration (CORS)	Low	Not Fixed
Improper CSRF token handling	Low	Not Fixed
Broken Authentication	Low	Not Fixed
Broken IDOR Protection (Denial of Service)	Low	Not Fixed

3 GENERAL RECOMMENDATIONS

This section contains general recommendations how to fix discovered during the testing weaknesses and vulnerabilities and how to improve overall security level.

For the current weaknesses remediation, follow the guidelines in the full technical report.

The following recommendations have been given to the Customer during initial information gathering and consulting sessions. The Customer followed the recommendations and started to build mature security process and regular security tests.

1. Set up a regular software update routine,
2. Constantly monitor public bug trackers to quickly fix vulnerabilities in the third-party software,
3. Regularly perform code review of the developed software,
4. Regularly perform black box vulnerability scanning,
5. Regularly perform network infrastructure inventory,
6. Use strict password policy,
7. Adopt the secure configuration guidelines and standards. Useful websites:: http://cisecurity.org, http://www.sans.org, http://www.nist.gov.
8. Adopt the secure development best practices. Useful website for secure web application development: http://www.owasp.org