Secure Code Review

Findings and Recommendations Report Presented to:

Client name.

August 19, 2022

Version: 1.0

Presented by:

Kudelski Security, Inc.

5090 North 40th Street, Suite 450

Phoenix, Arizona 85018

STRICTLY CONFIDENTIAL

# TABLE OF CONTENTS

[TABLE OF CONTENTS 2](#_Toc111737202)

[LIST OF FIGURES 2](#_Toc111737203)

[LIST OF TABLES 2](#_Toc111737204)

[EXECUTIVE SUMMARY 3](#_Toc111737205)

[Overview 3](#_Toc111737206)

[Key Findings 3](#_Toc111737207)

[Scope and Rules Of Engagement 4](#_Toc111737208)

[TECHNICAL ANALYSIS & FINDINGS 5](#_Toc111737209)

[Findings 6](#_Toc111737210)

[KS-01 Lack of mechanism to protect Reward ATA’s funds 7](#_Toc111737211)

[KS-02 Improper Access Control for Register Stake Instruction 10](#_Toc111737212)

[KS-03 Integer not properly documented in mathematical operation 12](#_Toc111737213)

[METHODOLOGY 14](#_Toc111737214)

[Tools 15](#_Toc111737215)

[Vulnerability Scoring Systems 16](#_Toc111737216)

[KUDELSKI SECURITY CONTACTS 18](#_Toc111737217)

# LIST OF FIGURES

[Figure 1: Findings by Severity 6](#_Toc107578886)

# LIST OF TABLES

[Table 1: Scope 5](#_Toc107578883)

[Table : Findings Overview 7](#_Toc107578884)

# EXECUTIVE SUMMARY

## Overview

Client-name-here engaged Kudelski Security to perform a code review of the programs-name-here programs.

The assessment was conducted remotely by the Kudelski Security Team. Testing took place between starting-date-here and ending-date-here, and it was focused on the following objectives:

* Provide the customer with an assessment of their overall security posture and any risks that were discovered within the environment during the engagement.
* To provide a professional opinion on the maturity, adequacy, and efficiency of the security measures that are in place.
* To identify potential issues and include improvement recommendations based on the result of our tests.

During the Secure Code Review, we identified count-findings-here findings according to our Vulnerability Scoring System.

This report summarizes the engagement, tests performed, and details of the mentioned findings.

It also contains detailed descriptions of the discovered vulnerabilities, steps the Kudelski Security Teams took to identify and validate each issue,as well as any applicable recommendations for remediation.

## Key Findings

The following are the major themes and issues identified during the testing period.

These, along with other items, within the findings section, should be prioritized for remediation to reduce to the risk they pose.

* Key-finding-1
* Key-finding-2
* Key-finding-3
* Key-finding-4

## 

## Scope and Rules Of Engagement

Kudelski performed a Secure Code Review for client-name-here. The following table documents the targets in scope for the engagement. No additional systems or resources were in scope for this assessment.

|  |  |
| --- | --- |
| **Commit Hash** | |
| commit-hash here | |
| **In-Scope Repositories** | |
| repository-name-here | Description of repository here |
| **In-Scope Contracts – Program Name** | |
| file-name-1.rs | file-name-2.rs |
| file-name-3.rs | file-name-4.rs |
| … | …. |
|  |  |
|  |  |
|  |  |
|  |  |

Table 1: Scope

# TECHNICAL ANALYSIS & FINDINGS

During the Secure Code Review, we identified count-findings-here findings according to our Vulnerability Scoring System.

The following chart displays the findings by severity.

Figure 1: Findings by Severity

## Findings

The *Findings* section provides detailed information on each of the findings, including methods of discovery, explanation of severity determination, recommendations, and applicable references.

The following table provides an overview of the findings.

|  |  |  |
| --- | --- | --- |
| **#** | **Severity** | **Description** |
| 1 | **Medium** | Example 1 |

Table 2: Findings Overview

## KS-01 Example

|  |  |
| --- | --- |
| Severity | **Medium** |

|  |  |  |
| --- | --- | --- |
| **Impact** | **Likelihood** | **Difficulty** |
| High | Low | High |

**Description**

**Impact**

**Evidence**

**Affected Resource**

**Recommendation**

**Reference**

# METHODOLOGY

During this source code review, the Kudelski Security Services team reviewed code within the project within an appropriate IDE. During every review, the team spends considerable time working with the client to determine correct and expected functionality, business logic, and content to ensure that findings incorporate this business logic into each description and impact. Following this discovery phase the team works through the following categories:

* Authentication
* Authorization and Access Control
* Injection and Tampering
* Configuration Issues
* Logic Flaws
* Cryptography

### Tools

The following tools were used during this portion of the test. A link for more information about the tool is provided as well.

* Visual Studio Code
* Semgrep
* Cargo Audit

## Vulnerability Scoring Systems

Kudelski Security utilizes a vulnerability scoring system based on impact of the vulnerability, likelihood of an attack against the vulnerability, and the difficulty of executing an attack against the vulnerability based on a high, medium, and low rating system

**Impact**

The overall effect of the vulnerability against the system or organization based on the areas of concern or affected components discussed with the client during the scoping of the engagement.

**High:**

The vulnerability has a severe affect on the company and systems or has an affect within one of the primary areas of concern noted by the client

**Medium:**

It is reasonable to assume that the vulnerability would have a measurable affect on the company and systems that may cause minor financial or reputational damage.

**Low:**

There is little to no affect from the vulnerability being compromised. These vulnerabilities could lead to complex attacks or create footholds used in more severe attacks.

**Likelihood**

The likelihood of an attacker discovering a vulnerability, exploiting it, and obtaining a foothold varies based on a variety of factors including compensating controls, location of the application, availability of commonly used exploits, and institutional knowledge

**High:**

It is extremely likely that this vulnerability will be discovered and abused

**Medium:**

It is likely that this vulnerability will be discovered and abused by a skilled attacker

**Low:**

It is unlikely that this vulnerability will be discovered or abused when discovered.

**Difficulty**

Difficulty is measured according to the ease of exploit by an attacker based on availability of readily available exploits, knowledge of the system, and complexity of attack. It should be noted that a LOW difficulty results in a HIGHER severity.

**Low:**

The vulnerability is easy to exploit or has readily available techniques for exploit

**Medium:**

The vulnerability is partially defended against, difficult to exploit, or requires a skilled attacker to exploit.

**High:**

The vulnerability is difficult to exploit and requires advanced knowledge from a skilled attacker to write an exploit

**Severity**

Severity is the overall score of the weakness or vulnerability as it is measured from Impact, Likelihood, and Difficulty

# KUDELSKI SECURITY CONTACTS

|  |  |  |
| --- | --- | --- |
| **NAME** | **POSITION** | **CONTACT INFORMATION** |
| **Auditor 1** | **Blockchain Security Expert** | **name.lastname@kudelskisecurity.com** |
| **Auditor 2** | **Blockchain Security Analyst** | **name.lastname@kudelskisecurity.com** |
| **Auditor 3** | **Blockchain Security Expert** | **name.lastname@kudelskisecurity.com** |