Guard

Smart contracts security assessment

Final report

Tariff: Standard

Red pill

April 2022

0xguard.com

hello@0xguard.com

Contents

Introduction

The report has been prepared for Red pill project team.

The audited scope includes the staking contract and a new version of the revenue calculator. The contract imports comprise an Anchor framework that currently is in an active development phase. The project's team and potential users should consider possible security breaches in the early framework versions that can not be revealed during the audit.

Name	Red pill
Audit date	2022-04-24 - 2022-04-29
Language	Rust
Platform	Solana

Contracts checked

Name	Address
lib.rs	3XbnCcEzq7ANVfm1y81Km9L4wZBdRPvMfyX16iUs4A3N
pool_v2.rs	
mod.rs	
version.rs	

Procedure

We perform our audit according to the following procedure:

Automated analysis

- Scanning the project's smart contracts with several publicly available automated Rust and Solana analysis tools
- Manual verification (reject or confirm) all the issues found by the tools

Manual audit

- Manually analyse smart contracts for security vulnerabilities
- Smart contracts' logic check

Known vulnerabilities checked

Title	Check result
Missing ownership check	passed
Missing signer check	passed
Integer overflow & underflow	passed
Arbitrary signed program invocation	passed
Solana account confusions	passed

Classification of issue severity

High severity	High severity issues can cause a significant or full loss of funds, change of contract ownership, major interference with contract logic. Such issues require immediate attention.
Medium severity	Medium severity issues do not pose an immediate risk, but can be detrimental to the client's reputation if exploited. Medium severity issues may lead to a contract failure and can be fixed by modifying the contract state or redeployment. Such issues require attention.
Low severity	Low severity issues do not cause significant destruction to the contract's functionality. Such issues are recommended to be taken into consideration.

Issues

High severity issues

No issues were found

Medium severity issues

No issues were found

Low severity issues

No issues were found

Conclusion

Red pill lib.rs, pool_v2.rs, mod.rs, version.rs contracts were audited. No severity issues were found.

The project uses the Anchor framework, that is widely used but is still under active development.

Disclaimer

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability)set forth in the Services Agreement, or the scope of services, and terms and conditions provided to the Company in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes without 0xGuard prior written consent.

This report is not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any “product” or “asset” created by any team or project that contracts 0xGuard to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Soteria scanner result

```
Analyzing /workspace/programs/staking/.coderrect/build/bpfel-unknown-unknown/release/
all.ll ...

Cargo.toml: spl_token version: 3.3.0

anchor_lang_version: 3.3.0 anchorVersionTooOld: 0

Cargo.toml: anchor_lang version: 0.24.2

anchor_lang_version: 0.24.2 anchorVersionTooOld: 0

 - ⠁ [00m:01s] Loading IR From File

 - ⠁ [00m:00s] Running Compiler Optimization Passes

EntryPoints:

entrypoint

 - ⠁ [00m:00s] Running Compiler Optimization Passes

 - ⠁ [00m:00s] Running Pointer Analysis

 - ⠁ [00m:00s] Building Static Happens-Before Graph

 - ⠁ [00m:00s] Detecting Vulnerabilities

detected 0 untrustful accounts in total.

detected 0 unsafe math operations in total.

--------The summary of potential vulnerabilities in all.ll--------

        No vulnerabilities detected
```

0x Guard