Date: 24.03.2023

Security Audit

PAPASALE LAUNCHPAD

Harry.K

Harry Kedelman

General Manager

Conclusion

PAPASALE LAUNCHPAD Platform has successfully PASSED the security audit

(Other unknown security vulnerabilities are not included in the audit responsibility scope)

Overall Test Result

OVERAL REVIEW		Code Quality Assesment	Manual Audit & Test	Automated Test	Functionality Test	Integrated Test
Airdrop System	Airdrop.sol	Passed	Passed	Passed	Passed	Passed
	AirdropFactory.sol	Passed	Passed	Passed	Passed	Passed
	AirdropManager.sol	Passed	Passed	Passed	Passed	Passed
Launchpad Contracts	PoolFactory.sol	Passed	Passed	Passed	Passed	Passed
	PoolFactoryManager.sol	Passed	Passed	Passed	Passed	Passed
	PoolFairlaunch.sol	Passed	Passed	Passed	Passed	Passed
	PoolFairlaunchFactory.sol	Passed	Passed	Passed	Passed	Passed
	PoolPresale.sol	Passed	Passed	Passed	Passed	Passed
Token Locker System	Locker.sol	Passed	Passed	Passed	Passed	Passed

SWC Test Result

When the security vulnerabilities identified as a result of the SWC test are evaluated with integrated tests, it is verified that they are not of critical value to cause loss, and the project owner has been informed as necessary.

These Vulnerabilities are acknowledged as Informational level

SWC TEST RESULT		High	Medium	Low	Remission
Airdrop System	Airdrop.sol	0	0	7	Acknowledged
	AirdropFactory.sol	0	3	10	Acknowledged
	AirdropManager.sol	0	0	1	Acknowledged
Launchpad Contracts	PoolFactory.sol	0	0	1	Acknowledged
	PoolFactoryManager.sol	0	0	2	Acknowledged
	PoolFairlaunch.sol	0	0	4	Acknowledged
	PoolFairlaunchFactory.sol	0	0	6	Acknowledged
	PoolPresale.sol	0	0	2	Acknowledged
Token Locker System	Locker.sol	0	0	4	Acknowledged

Table of Contents

SUMMARY

This report has been prepared for Papasale Launchpad Platform of to discover issues and vulnerabilities in the source code of overall Launch platform as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Static Analysis and Manual Review techniques.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

The security assessment resulted in findings that ranged from critical to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices. We suggest recommendations that could better serve the project from the security perspective:

- Enhance general coding practices for better structures of source codes.
- Add enough unit tests to cover the possible use cases.
- Provide more comments per each function for readability, especially contracts that are verified in public.
- Provide more transparency on privileged activities once the protocol is live.

OVERVIEW

Project Summary

Project Name	Papasale
Audited Feature	All features, and contract used for launchpad
Platform	Multichain
Language	Solidity
Audited Contracts:	
Airdrop.sol	
AirdropFactory.sol	
AirdropManager.sol	
PoolFactory.sol	
PoolFactoryManager.sol	
PoolFairlaunch.sol	
PoolFairlaunchFactory.sol	
PoolPresale.sol	
Locker.sol	

Audit Summary

Delivery Date	March 24, 2023
Audit Methodology	Static Analysis, Manual Review, Automated Test
Key Components	Papasale

Auditing Approach and Applied Methodologies

The auditing process pays special attention to the following considerations:

- Code design patterns analysis in which smart contract architecture is reviewed to ensure it is structured according to industry standards and safe use of third-party smart contracts and libraries.
- Line-by-line inspection of the Smart Contract to find any potential vulnerability like race conditions, transaction-ordering dependence, timestamp dependence, and denial of service attacks.
- Unit testing Phase, we coded/conducted custom unit tests written for each function in the contract to verify that each function works as expected.
- Automated Test performed with our in-house developed tools to identify vulnerabilities and security flaws of the Smart Contract.

Security
Identifying security related issues within each contract and the system of contract.

Sound Architecture
Evaluation of the architecture of this system through the lens of established smart contract best practices and general software best practices.

Code Correctness and Quality
A full review of the contract source code. The primary areas of focus include:
- Accuracy
- Readability
- Sections of code with high complexity
- Quantity and quality of test coverage

Smart Contract SWC Attack Test

Airdrop.pdf

AirdropFactory.pdf

AirdropManager.pdf

PoolFactory.pdf

PoolFactoryManager.pdf

PoolFairlaunch.pdf

PoolFairlaunchFactory.pdf

PoolPresale.pdf

Locker.pdf

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. To get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us based on what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and ContractChecker and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (ContractChecker) owe no duty of care towards you or any other person, nor does ContractChecker make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and ContractChecker hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, ContractChecker hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against ContractChecker, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.