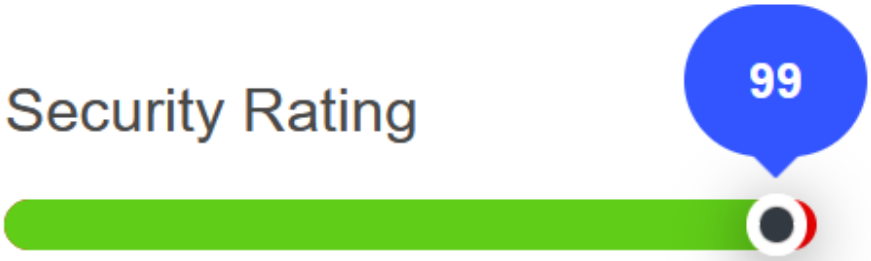
SECURICHAIN

SMART CONTRACT SECURITY ANALYSIS REPORT ON

REDKITE

Jan 27th 2022



(The rating is based on the number, severity and latest status of detected issues)

Disclaimer

This report containings confidential information which can be used internally by the Customer, or it can be disclosed publicly after all vulnerabilities are fixed — upon a decision of the Customer.

SecuriChain does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed.

The report in no way provide investment advice, nor should be leveraged as investment advice of any sort.

TABLE OF CONTENTS

1. VULNERABILITY ASSESSMENT OVERVIEW

1.1. ASSIGNING RISK LEVELS

The Auditor categorizes each of the detected vulnerabilities into 4 levels (**High**, **Medium**, **Low**, and **Info**) according to the degree of the risks it may cause in Customer's operations. For details of the rating standards, please refer to "Appendix 2 Risk Rating." Please also note that the assessment of the findings is based on Auditor's own perspective and may contain speculations in some cases.

1.2. SCOPE OF WORK

Project Name	REDKITE
Platform	ETHEREUM
Languages	SOLIDITY
Methods	AUTOMATION SCAN, ARCHITECTURE REVIEW, FUNCTIONAL TESTING, MANUAL CODE REVIEW
Repository	GITHUB: HTTPS://GITHUB.COM/POLKAFOUNDRY/REDKITE-CONTRACT COMMIT: A75BCEC
Documents	
Timelines	**JAN 18TH 2022 – JAN 27TH 2022**

1.3. CHECKSUM FILE

REDKITE – IDO-POOL

No.	Hash	Name
1	828d640d61774e6d72b025ae8f1842b76b0f69bfd884e73003178d84155b87a4	RedKiteWhitelist.sol
2	0573c2961569aa4906845d0cd428b5b7394956170054ceeaa8f8af96cd44875c	IERC20.sol
3	a0a7b29dacc4e94925b572546a10e5278aab549691f69b55ebefbe5333a87f6c	IPoolFactory.sol
4	0c75c8c096be3622e1f1d9fc7debd21ddbe64cbacec5d9f502d7a1b6dd1a482f	IPool.sol
5	bd32c2c07d6468f850437b5376499e01db196a6f682b9139ca6e27d6bbbb4be9	Initializable.sol
6	dffd33051e6e06e2927a2a92d144049a24f6dbf5ba30b73eb7346df43d9abdff	Ownable.sol
7	203919d034da2078536b842856d6697edbb2aad6fa9794a23285f3d715619a0f	Pausable.sol
8	e45d05561ed23ccf15fd12dc4e3b4c7f75839f9a18af3063ebed37b332d3da85	ReentrancyGuard.sol
9	670c634cfe13c61ba10b6fb7c48e7ea886f2a693c17a39986d9f22abcd5b6290	SafeMath.sol
10	27cecf9765195e7f3a7eea2e010ad5af4cf69c7c3289f498afdf2010c728736f	TransferHelper.sol
11	110c086f3b969b5d89f8b46e8a3522e8bc5123654fed2ff83b24dd1e3f18245b	PreSaleFactory.sol
12	f85d095adb73fbe22bea4510cb8d6416390e59a59263b31d86d48773e34c2f36	PreSalePool.sol

REDKITE – STAKING

No.	Hash	Name
1	d823bb915bc0442e8efb01052946f8a7cd0b517b6702a1005f749b1b03de296d	AllocationPool.sol
2	b79faa3b002d4912be2a23a7daca121ee372707cf8ee9373e2a1c4b163f3dd87	LinearPool.sol
3	fd5beabaa4cff5c3a94ece8d8584f774e6404528182824971bef06ca506d35fc	StakingPool.sol
4	c2ebd8a6011b1fca46df37ea5b9d0c428af0f00c0f1c34a1dc7ee5911a1cc022	ERC20Mock.sol

1.4. ASSESSMENT RESULTS

According to the assessment, the Customer's smart contracts have the security rating of 99/100

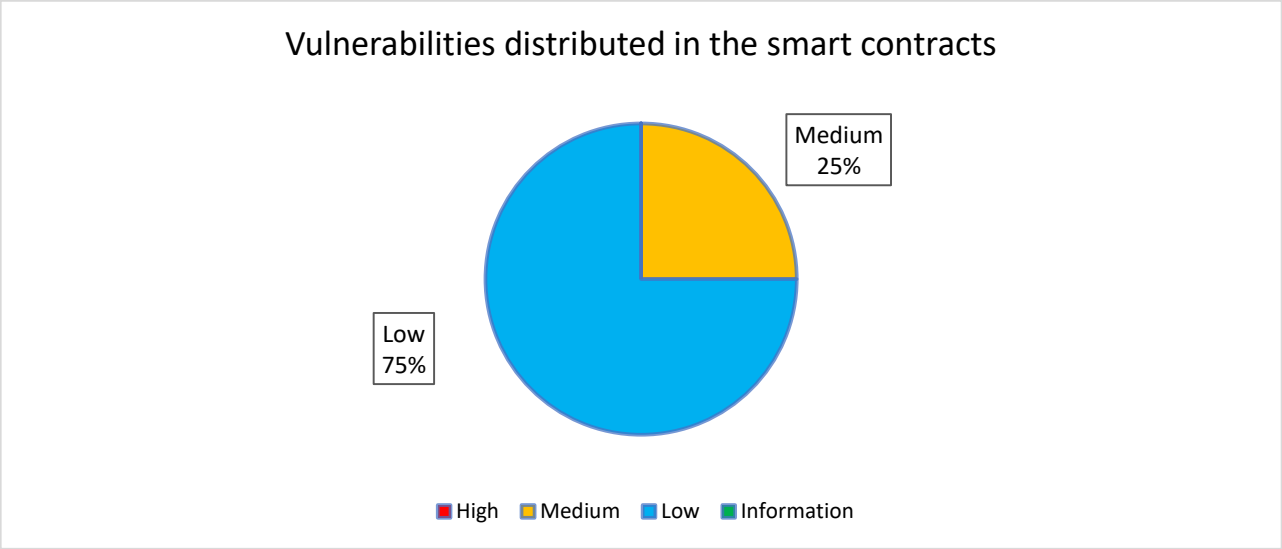
Rate	Description
90-100	**No vulnerabilities** were found or all detected ones have been resolved
60-89	Unresolved **Low-level** vulnerabilities exist
40-59	Unresolved **Medium-level** vulnerabilities exist
0-39	Unresolved **High-level** vulnerabilities exist

(For more information on criteria for risk rating, refer to Appendix.2)

2. FINDINGS

2.2. LIST OF VULNERABILITIES

The detected vulnerabilities are listed below. Please refer to "Appendix.2 Risk Rating" for the risk assessment method.



ID	Risk Level	Name	Amount	Status *(after re-checking)*
SC1	Medium	The allocClaimAll () function does not work as expected.	1	Resolved in commit id: 35c8aa15846df5df40c1ddf20182988633ee48c2
SC2	Low	Gas Optimization	3	Resolved in commit id: e18fa03062ef71a26f3b106cb1fd9ee7f317eb43

(For rating of each vulnerability, refer to Appendix 2.)

2.3. DETAILS

[1] Function does not work as expected.

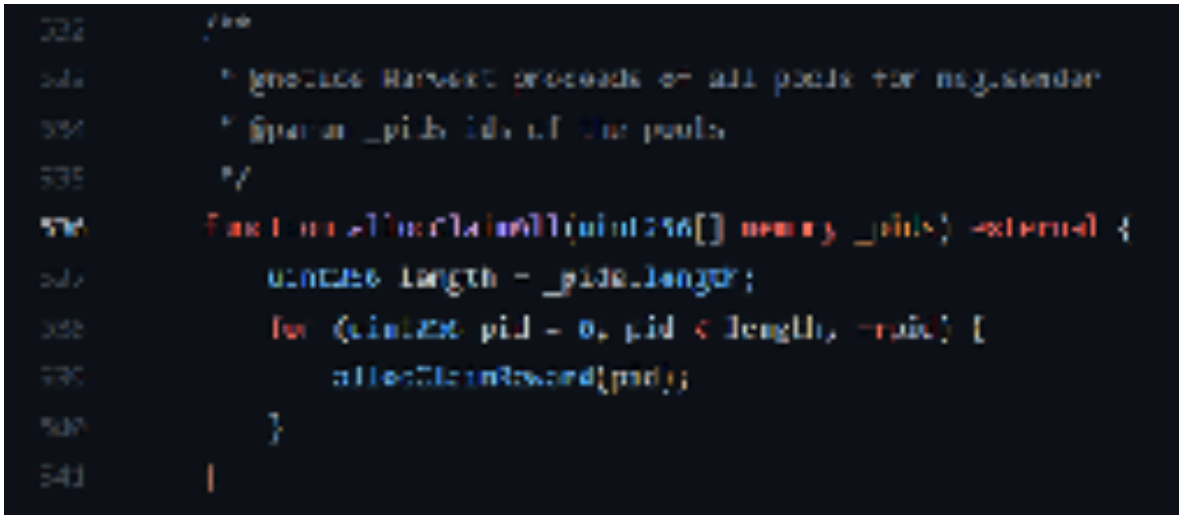
1 MEDIUM

- **Overview**

  Logic Vulnerability.

- **Description**

  The function is mishandling the `for` loop. The value in the _pids array is not used.



(Blurring the image of the code snippet in the public report because the Customer's code is in the private repository)

- **Recommendation**

  Use the value in the _pids array which corresponds to the index instead of using the index as a parameter to pass to the subfunction

- **Location:**
  - Staking::AllocationPool.sol (#L536-L541)

[2] Gas Optimization

3 LOW

- **Overview**

Gas optimization is a matter of doing what is cheap and avoiding what is expensive in terms of gas costs on EVM blockchains.

- **Possible Impact**

(Blurring the image of the code snippet in the public report because the Customer's code is in the private repository)

Users have to pay more gas for their requests.

- **Recommendation**

Use ‘external’ instead of ‘public’ for functions that are only called outside of the contract.

- **Location:**
  - IDO-pool::PreSalePool.sol (#L299-L332, #L268-L297, #L363-L383)

3. CONCLUSION

This document, and its appendices, represents the results of several days of our intensive work.

Smart contracts within the scope were analyzed with static analysis tools and manually reviewed.

Please feel free to direct any questions on this assessment to: audit@securichain.io.

APPENDIX 1. ASSESSMENT LIST

CHECKLIST		
Arithmetic operations		
	Integer Overflow/Underflow	Integer Division
	Integer Truncation	Integer Sign
	Wrong Operator	
Re-entrancy		
Bad Randomness		
	Timestamp Dependence	Blockhash
Front running		
DDos		
	DOS By Complex Fallback Function	DOS By Gaslimit
	DOS By Non-existent Address Or Malicious Contract	
Unsafe external calls		
Gas usage		
	Invariants in Loop	Invariants State Variables Are Not Declared Constant
Business Logics Review		
Access Control & Authorization		
	Replay Attack	Use tx.origin For Authentication
Logic Vulnerability		

APPENDIX 2. RISK RATING

Risk Level	Explain	Example Types
High	The issue puts a large number of users' sensitive information at risk, or is reasonably likely to lead to catastrophic impact for client's reputation or serious financial implications for client and users.	Re-entrancy
		Front running
		DDos
		Bad Randomness
		Logic Vulnerability
		Arithmetic operations
Medium	The issue puts a subset of users' sensitive information at risk, would be detrimental for the client's reputation if exploited, or is reasonably likely to lead to moderate financial impact.	Access Control
		Unsafe external calls
		Business Logics Review
		Logic Vulnerability
Low	The risk is relatively small and could not be exploited on a recurring basis, or is a risk that the client has indicated is low-impact in view of the client's business circumstances.	Gas usage
Info	The issue does not pose an immediate risk, but is relevant to security best practices or Defence in Depth.	Do not specify a specific version of Solidity

