HackSafe

Smart Contract Security Audit Report

SUN

May 2022

Security Status

★★★★½

www.hacksafe.io

Audit Details

Audited project
SUN

Deployer address
TRX6Q82wMqWNbCCiLqejbZe43wk1h1zJHm

Client contacts
Sun team

Blockchain
Tron chain

Website
https://sun.io/#/home

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. In order 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 on the basis of 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 any and 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 TechRate and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (HackSafe) owe no duty of care towards you or any other person, nor does HackSafe 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 HackSafe 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, HackSafe hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against HackSafe, 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.

Procedure

Step 1 - In-Depth Manual Review

Manual line-by-line code reviews to ensure the logic behind each function is sound and safe from various attack vectors. This is the most important and lengthy portion of the audit process (as automated tools often cannot find the nuances that lead to exploits such as flash loan attacks).

Step 2 - Automated Testing

Simulation of a variety of interactions with your Smart Contract on a test blockchain leveraging a combination of automated test tools and manual testing to determine if any security vulnerabilities exist.

Step 3 – Leadership Review

The engineers assigned to the audit will schedule meetings with our leadership team to review the contracts, any comments or findings, and ask questions to further apply adversarial thinking to discuss less common attack vectors.

Step 4 - Resolution of Issues

Consulting with the team to provide our recommendations to ensure the code's security and optimize its gas efficiency, if possible. We assist project team's in resolving any outstanding issues or implementing our recommendations.

Step 5 - Published Audit Report

Boiling down results and findings into an easy-to-read report tailored to the project. Our audit reports highlight resolved issues and any risks that exist to the project or its users, along with any remaining suggested remediation measures. Diagrams are included at the end of each report to help users understand the interactions which occur within the project.

Background

HackSafe was commissioned by SUN to perform an audit of smart contract:

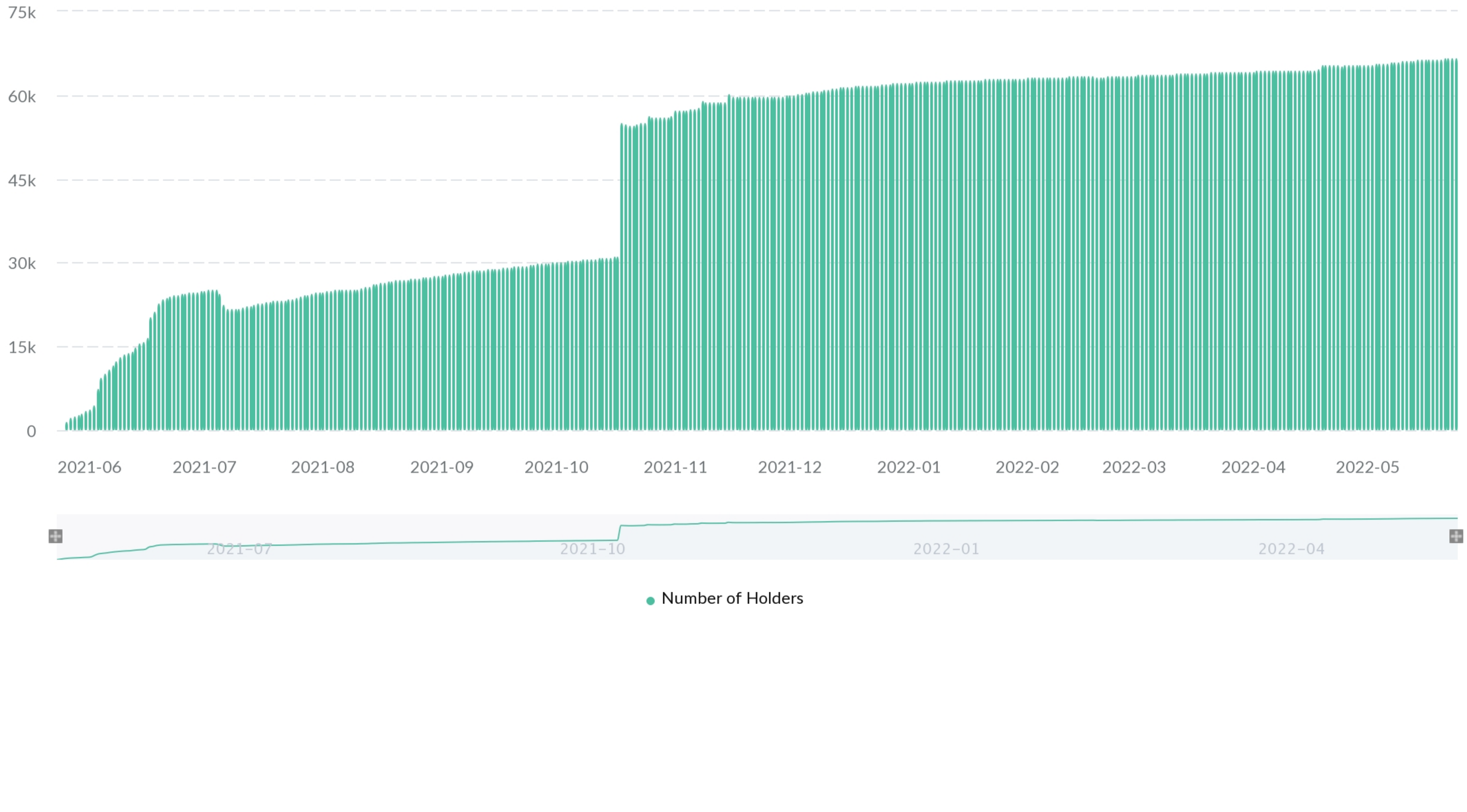
- https://tronscan.org/#/contract/TSSMHYeV2uE9qYH95DqyoCuNCzEL1NvU3S/code

Contract Details

Token contract details for 24.05.2022

Contract name	: SunToken
Contract address	: TSSMHYeV2uE9qYH95DqyoCuNCzEL1NvU3S
Compiler version	: solidity 0.5.8
Circulation supply	: 10,514,908,025
Total supply	: 19,900,730,000
Token Ticker	: SUN
Decimals	: 18
Token Holders	: 66,794
Transactions count	: 1,245,912
Contract deployer address	: TRX6Q82wMqWNbCCiLqejbZe43wk1h1zJHm
owner address	: No Owner

SUN Token Distribution



SUN Token Distribution

SUN Top 20 Token Holders

Holders' Address

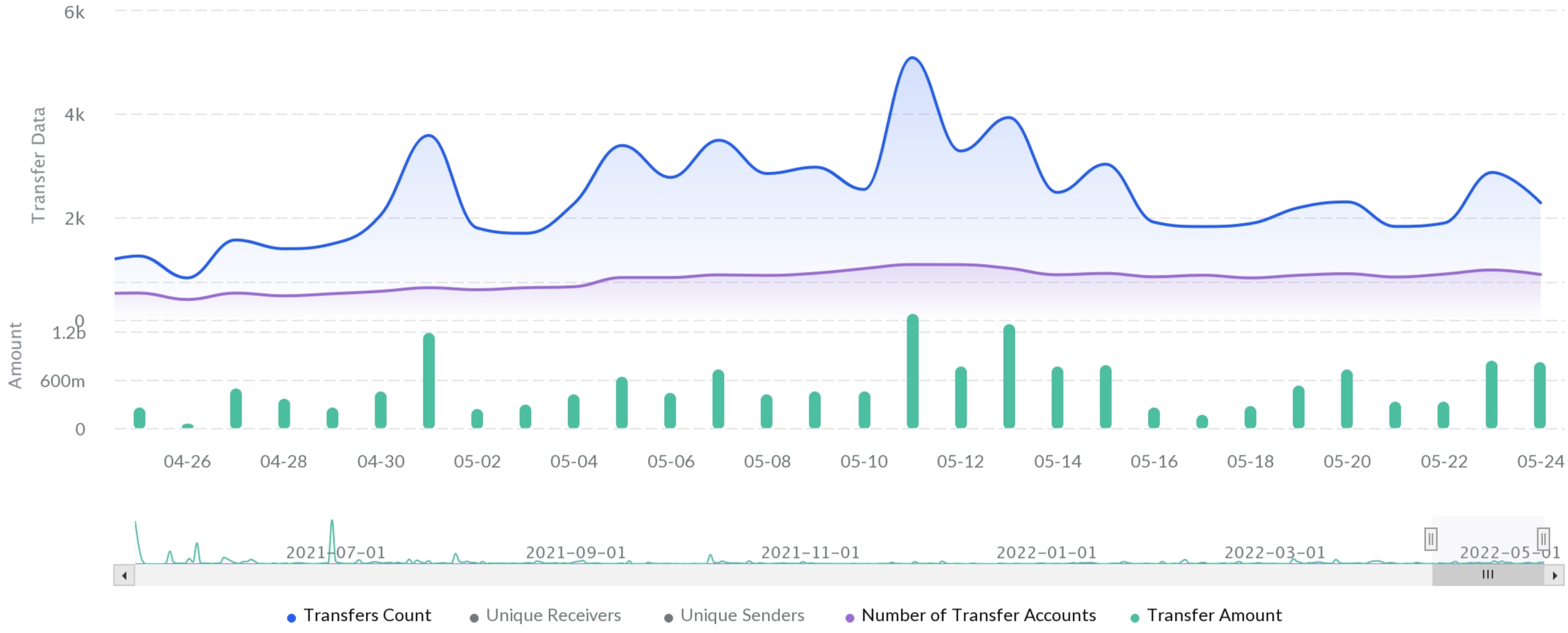
The latest 10,000 records of a total of 66,797 addresses are shown here.

Search Address

Rank	Address		Amount	Value	Percentage
1	TEPMzyy5Qo9vP5g24ACo1o7wquyQxRC1xY		10,432,893,597.432429772467171840	$97,575,132.6	52.424678%
2	SC TSB5XcidLZUBRHd2sMbUZ1LLQ...UFtuF		2,190,159,073.338803058614023000	$20,483,776.62	11.005421%
3	SC TXbA1feyCqWAfAQgXvN1ChTg... T8QPb		1,086,629,051.216991227584857136	$10,162,853.94	5.460247%
4	SC TDQaYrhQynYV9aXTYj63nwLAa... WSEj6		1,085,724,248.205963487182352647	$10,154,391.64	5.455701%
5	SC TPXDpkg9e3eZzxqxAUyke9S4z4... BJw9e		991,470,618.184994482842824108	$9,272,871.05	4.982082%
6	SC TU2sYRRA1QsdV5yuSLxRRfyLZ... NMYry		752,630,773.615860247833989725	$7,039,087.18	3.781925%
7	TWd4WrZ9wn84f5x1hZhL4DHvk738ns5jwb	Bi...	700,000,000.000000000000000000	$6,546,850.32	3.517459%
8	THQFoJSwtsMMRKCG6B7P5kGcxJQXGi2kiS	Bith...	324,459,549.196069600257331778	$3,034,554.44	1.63039%
9	TV6MuMXfmLbBqPZvBHdwFsDnQeVfnmiuSi	Bi...	296,280,783.583108930000000000	$2,771,008.49	1.488794%
10	TA9FnQrLGdgLW6cwBKue9DyqSBz1UNzUMR	Upbit	214,416,700.906415961344603741	$2,005,362.93	1.077431%
11	TM1zzNDZD2DPASbKcgdVoTYhfmYgtfwx9R	O...	209,396,050.452993071262760000	$1,958,406.57	1.052203%
12	SC TTdeCobmYxhfFBYUZbiQqbZ56... SE5DG		167,920,782.903046269666919296	$1,570,503.19	0.843792%
13	TPyjyZfsYaXStgz2NmAraF1uZcMtkgNan5		159,000,692.938750485873558723	$1,487,076.77	0.798969%
14	TNaRAoLUyYEV2uF7GUrzSjRQTU8v5ZJ5VR	H...	158,887,044.826601591796294562	$1,486,013.86	0.798398%
15	TMuA6YqfCeX8EhbfYEg5y7S4DqzSJireY9	Bi...	100,000,000.000000000000000000	$935,264.33	0.502494%
16	SC TJvd6BKZUayxVUtecRF9CFqA85... gqux4		65,400,106.424909050689403839	$611,663.87	0.328632%
17	TWUbdjYDeoSE9wj59vcTK33hFiHf4sVpoK		53,801,988.828356809391042063	$503,190.81	0.270352%
18	TNXoiAJ3dct8Fjg4M9fkLFh9S2v9TXc32G	Bi...	51,778,930.418992910000000000	$484,269.87	0.260186%
19	SC THu6ConqvZ3phYHeNTDyW9aE...wBsP6		51,255,695.944824612960362062	$479,376.24	0.257557%
20	TNCmcTdyrYKMtmE1KU2itzeCX76jGm5Not	P...	47,639,428.165115985607263327	$445,554.58	0.239385%

SUN Token Distribution

SUN Token Transfer Data



Contract functions details

BaseTRC20.sol
+ BaseTRC20 (Context, ITRC20)
    -[Pub] totalSupply
    -[Pub] balanceOf
    -[Pub] transfer
    -[Pub] allowance
    -[Pub] approve
    -[Pub] transferFrom
    -[Pub] increaseAllowance#
    -[Pub] decreaseAllowance#
    - [Int] _transfer #
    - [Int] _mint #
    - [Int] _burn #
    - [Int] _approve #

+TRC20Detailed (BaseTRC20)
    -[Pub] <constructor> #
    - [Pub] name
    - [Pub] symbol
    -[Pub] decimals

Context.sol
+Context
    -[Int] <constructor>
    -[Int] _msgSender

ITRC20.sol
+ TRC20Events
+ ITRC20 (TRC20Events)
    -[Ext] totalSupply
    -[Ext] balanceOf
    -[Ext] allowance
    -[Ext] approve
    -[Ext] transfer
    -[Ext] transferFrom

Contract functions details

SafeMath.sol
+ SafeMath
    -[Int] add
    -[Int] sub
    -[Int] mul
    -[Int] div
    -[Int] div
    -[Int] mod
    -[Int] mod

SunToken.sol
+ SunToken (ITRC20, TRC20Detailed)
    -[Pub] <constructor> #

($) = payable function
= non-constant function

Issues Checking Status

No.	Title	Status
1.	Unlocked Compiler Version	Low issue
2.	Missing Input Validation	Passed
3.	Race conditions and Reentrancy. Cross-function race conditions.	Passed
4.	Possible delays in data delivery	Passed
5.	Oracle calls.	Passed
6.	Timestamp dependence.	Passed
7.	Integer Overflow and Underflow	Passed
8.	DoS with Revert.	Passed
9.	DoS with block gas limit.	Passed
10.	Methods execution permissions.	Passed
11.	Economy model of the contract.	Passed
12.	Private use data leaks.	Passed
13.	Malicious Event log.	Passed
14.	Scoping and Declarations.	Passed
15.	Uninitialized storage pointers.	Passed
16.	Arithmetic accuracy.	Passed
17.	Design Logic.	Passed
18.	Safe Open Zeppelin contracts implementation and usage.	Passed
19.	Incorrect Naming State Variable	Passed

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to assets loss or data manipulations.
High	High-level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g., public access to crucial functions
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to assets loss or data manipulations.
Low	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that can't have a significant impact on execution.

Security Issues

- **Critical Severity Issues**
  No critical severity issue found.

- **High Severity Issues**
  No high severity issue found.

- **Medium Severity Issues**
  No medium severity issues found.

- **Low Severity Issues**
  One low severity issue found.

1. Unlocked Compiler Version.

- **Description**

  The contract utilizes an unlocked compiler version. An unlocked compiler version in the contract's source code permits the user to compile it at or above a particular version. This, in turn, leads to differences in the generated bytecode between compilations due to differing compiler version numbers. This can lead to ambiguity when debugging as compiler-specific bugs may occur in the codebase that would be difficult to identify over a span of multiple compiler versions rather than a specific one.

- **Recommendation**

  It is advisable that the compiler version is alternatively locked at the lowest version possible so that the contract can be compiled. For example, for version ^0.5.8 the contract should contain the following line:

  pragma solidity 0.5.8;

Conclusion

Smart contract contains low severity issues! The further transfer and operations with the fund raised are not related to this particular contract.

HackSafe note: Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.