



SOLIDProof
Bring trust into your projects

**Blockchain Security | Smart Contract Audits | KYC
Development | Marketing**

MADE IN GERMANY

Kommunitas

AUDIT

SECURITY ASSESSMENT

30. October, 2023

FOR



SolidProof_io



@solidproof_io

Introduction	4
Disclaimer	4
Project Overview	5
Summary	5
Social Medias	6
Audit Summary	6
File Overview	7
Imported packages	8
Audit Information	9
Vulnerability & Risk Level	9
Auditing Strategy and Techniques Applied	10
Methodology	10
Overall Security	11
Upgradeability	11
Ownership	12
Ownership Privileges	13
Minting tokens	13
Burning tokens	14
Blacklist addresses	15
Fees and Tax	16
Lock User Funds	17
Components	18
Exposed Functions	18
StateVariables	18
Capabilities	19
Inheritance Graph	20
Centralization Privileges	21
Audit Results	24
Critical issues	24
High issues	24



Medium issues	25
Low issues	26
Informational issues	27



Introduction

[SolidProof.io](#) is a brand of the officially registered company MAKE Network GmbH, based in Germany. We're mainly focused on Blockchain Security such as Smart Contract Audits and KYC verification for project teams.

Solidproof.io assess potential security issues in the smart contracts implementations, review for potential inconsistencies between the code base and the whitepaper/documentation, and provide suggestions for improvement.

Disclaimer

[SolidProof.io](#) reports are not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. These reports are not, nor should be considered, an indication of the economics or value of any “product” or “asset” created by any team. SolidProof.io do not cover testing or auditing the integration with external contract or services (such as Unicrypt, Uniswap, PancakeSwap etc'...)

SolidProof.io Audits do not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technology proprietors. SolidProof Audits should not be used in any way to make decisions around investment or involvement with any particular project. These reports in no way provide investment advice, nor should be leveraged as investment advice of any sort.

SolidProof.io Reports represent an extensive auditing 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. Blockchain technology and cryptographic assets present a high level of ongoing risk. SolidProof's position is that each company and individual are responsible for their own due diligence and continuous security. SolidProof in no way claims any guarantee of the security or functionality of the technology we agree to analyze.

Project Overview

Summary

Project Name	Kommunitas
Website	https://kommunitas.net
About the project	Kommunitas is a decentralized crowdfunding ecosystem for web3.0 projects. Some might refer to it as a "launchpad" or "IDO Platform" but Kommunitas is aiming to build not only a platform, but more to an ecosystem.
Chain	Ethereum, BSC, Polygon
Language	Solidity
Codebase Link	<p>A. BSC</p> <p>Fixed : https://bscscan.com/address/0xbF0DCC47e58B80aFf68D291259B514A287EDE122</p> <p>Linear : https://bscscan.com/address/0x3ae03C030a272699e0C51505E4E599b4D2f8C863</p> <p>Refunder : https://bscscan.com/address/0xB352B0387E83c5dbD846F098975606E4b12f9392</p> <p>B. Polygon</p> <p>Fixed : https://polygonscan.com/address/0xbABcb76305Eda9C4bc768755B163F1845e80F747</p> <p>Linear : https://polygonscan.com/address/0xe4EEFA94172Ba4523E2154baa90c4A0c84c838a8</p> <p>Refunder : https://polygonscan.com/address/0x6C6332d639631374CdC07e8cAF21740491Dc8A9f</p> <p>C. ETH</p> <p>Fixed : https://etherscan.io/address/0x4056Ac1528C9cEA6668C1F578D9De86e8c9A6C2C</p> <p>Linear : https://etherscan.io/address/0x3B01591b66F4f8cCFEB409B6BD1467120069B7b4</p> <p>Refunder : https://etherscan.io/address/0x77ebEbf1De7B018b6678A224C66c1a645a0b5962</p>
Commit	N/A
Unit Tests	Provided

Social Medias

Telegram	https://t.me/Kommunitas_Ann
Twitter	https://twitter.com/kommunitas1
Facebook	https://facebook.com/kommunitas1/
Instagram	https://instagram.com/kommunitas1
Github	https://github.com/Kommunitas-net
Reddit	https://reddit.com/r/kommunitas
Medium	https://medium.com/@Kommunitas
Discord	https://discord.com/invite/hasFnzJbfp
Youtube	https://youtube.com/channel/UCBG6-Vj5KM-Xe5-PYtmV5Lg
TikTok	https://tiktok.com/@kommunitas.net
LinkedIn	https://linkedin.com/company/kommunitas-net/

Audit Summary

Version	Delivery Date	Changelog
v1.0	25. October 2023	<ul style="list-style-type: none"> • Layout Project • Automated- /Manual-Security Testing • Summary
v1.1	30. October 2023	<ul style="list-style-type: none"> • Reaudit

Note - The following audit report presents a comprehensive security analysis of the smart contract utilized in the project that includes outside manipulation of the contract's functions in a malicious way. This analysis did not include functional testing (or unit testing) of the contract/s logic. We cannot guarantee 100% logical correctness of the contract as we did not functionally test it. This includes internal calculations in the formulae used in the contract.



File Overview

The Team provided us with the files that should be tested in the security assessment. This audit covered the following files listed below with an SHA-1 Hash.

File Name	SHA-1 Hash
contracts/refunder/Refunder.sol	58e89862b855cf15f7ee700deea4cf189604a7bf
contracts/factory/RefunderFactory.sol	bc748c3676b2f739638b282f8f3fa3a379278199
contracts/factory/LinearVestingFactoryV2.sol	167b2dadcd3252fc04f775454ceedfcc6347d15
contracts/factory/FixedVestingFactoryV2.sol	892513e7571513eff5de007895b670b3e006f21d
contracts/vesting/LinearVestingV2.sol	8a917ee1a71b2d5d96bf42fd4c38293de608588f
contracts/vesting/FixedVestingV2.sol	4af191633a3473b3a1b3fcdcd602de25998ae482a

Please note: Files with a different hash value than in this table have been modified after the security check, either intentionally or unintentionally. A different hash value may (but need not) indicate a changed state or potential vulnerability that was not the subject of this scan.

Note for Investors: We only audited contracts mentioned in the scope above. Apart from that, all contracts related to the project are not a part of the audit, and we cannot comment on its security and are not responsible for it in any way.

Imported packages

Used code from other Frameworks/Smart Contracts (direct imports).

Dependency / Import Path	Count
@openzeppelin/contracts-upgradeable/access/ OwnableUpgradeable.sol	3
@openzeppelin/contracts-upgradeable/proxy/utils/Initializable.sol	7
@openzeppelin/contracts-upgradeable/proxy/utils/ UUPSUpgradeable.sol	3
@openzeppelin/contracts-upgradeable/security/ PausableUpgradeable.sol	6
@openzeppelin/contracts-upgradeable/token/ERC20/extensions/ IERC20MetadataUpgradeable.sol	3
@openzeppelin/contracts-upgradeable/token/ERC20/utils/ SafeERC20Upgradeable.sol	3
@openzeppelin/contracts/proxy/ERC1967/ERC1967Proxy.sol	1
@openzeppelin/contracts/proxy/beacon/BeaconProxy.sol	4
@openzeppelin/contracts/proxy/beacon/UpgradeableBeacon.sol	4

Audit Information

Vulnerability & Risk Level

Risk represents the probability that a certain source threat will exploit vulnerability and the impact of that event on the organization or system. The risk Level is computed based on CVSS version 3.0.

Level	Value	Vulnerability	Risk (Required Action)
Critical	9 - 10	A vulnerability that can disrupt the contract functioning in a number of scenarios, or creates a risk that the contract may be broken.	Immediate action to reduce risk level.
High	7 - 8.9	A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.	Implementation of corrective actions as soon as possible.
Medium	4 - 6.9	A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.	Implementation of corrective actions in a certain period.
Low	2 - 3.9	A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.	Implementation of certain corrective actions or accepting the risk.
Informational	0 - 1.9	A vulnerability that have informational character but is not effecting any of the code.	An observation that does not determine a level of risk

Auditing Strategy and Techniques Applied

Throughout the review process, care was taken to check the repository for security-related issues, code quality, and compliance with specifications and best practices. To this end, our team of experienced pen-testers and smart contract developers reviewed the code line by line and documented any issues discovered.

We check every file manually. We use automated tools only so that they help us achieve faster and better results.

Methodology

The auditing process follows a routine series of steps:

1. Code review that includes the following:
 - a. Reviewing the specifications, sources, and instructions provided to SolidProof to ensure we understand the size, scope, and functionality of the smart contract.
 - b. Manual review of the code, i.e., reading the source code line by line to identify potential vulnerabilities.
 - c. Comparison to the specification, i.e., verifying that the code does what is described in the specifications, sources, and instructions provided to SolidProof.
2. Testing and automated analysis that includes the following:
 - a. Test coverage analysis determines whether test cases cover code and how much code is executed when those test cases are executed.
 - b. Symbolic execution, which is analysing a program to determine what inputs cause each part of a program to execute.
3. Review best practices, i.e., review smart contracts to improve efficiency, effectiveness, clarity, maintainability, security, and control based on best practices, recommendations, and research from industry and academia.
4. Concrete, itemized and actionable recommendations to help you secure your smart contracts.



Overall Security

Upgradeability

Contract is an upgradeable

✗ Deployer can update the contract with new functionalities

Description

The deployer can replace the old contract with a new one with new features. Be aware of this, because the owner can add new features that may have a negative impact on your investments.

Example

We assume that you have funds in the contract and it has been audited by any security audit firm. Now the audit has passed. After that, the deployer can upgrade the contract to allow him to transfer the funds you purchased without any approval from you. This has the consequence that your funds can be taken by the creator.

Comment

N/A

Ownership

The ownership is not renounced

✗ The owner is not renounce

Description

The owner has not renounced the ownership that means that the owner retains control over the contract's operations, including the ability to execute functions that may impact the contract's users or stakeholders. This can lead to several potential issues, including:

- Centralizations
- The owner has significant control over contract's operations

Comment

N/A

Note - If the contract is not deployed, we would consider the ownership not renounced. Moreover, if there are no ownership functionalities, ownership is automatically considered renounced.



Ownership Privileges

These functions can be dangerous. Please note that abuse can lead to financial loss. We have a guide where you can learn more about these Functions.

Minting tokens

Minting tokens refer to the process of creating new tokens in a cryptocurrency or blockchain network. This process is typically performed by the project's owner or designated authority, who has the ability to add new tokens to the network's total supply.

Contract owner cannot mint new tokens

 **The owner cannot mint new tokens**

Description	The owner is not able to mint new tokens once the contract is deployed.
-------------	---

Comment	N/A
---------	-----



Burning tokens

Burning tokens is permanently destroying a certain number of tokens, reducing the total supply of a cryptocurrency or token. This is usually done to increase the value of the remaining tokens, as the reduced supply can create scarcity and potentially drive up demand.

Contract owner cannot burn tokens

 **The owner cannot burn tokens**

Description	The owner is not able burn tokens without any allowances.
-------------	---

Comment	N/A
---------	-----



Blacklist addresses

Blacklisting addresses in smart contracts is the process of adding a certain address to a blacklist, effectively preventing them from accessing or participating in certain functionalities or transactions within the contract. This can be useful in preventing fraudulent or malicious activities, such as hacking attempts or money laundering.

Contract owner cannot blacklist addresses



The owner cannot blacklist addresses

Description

The owner is not able blacklist addresses to lock funds.

Comment

N/A



Fees and Tax

In some smart contracts, the owner or creator of the contract can set fees for certain actions or operations within the contract. These fees can be used to cover the cost of running the contract, such as paying for gas fees or compensating the contract's owner for their time and effort in developing and maintaining the contract.

Contract owner cannot set fees more than 25%



The owner cannot levy unfair taxes

Description	The owner is not able to set the fees above 25%
Comment	N/A



Lock User Funds

In a smart contract, locking refers to the process of restricting access to certain tokens or assets for a specified period of time. When tokens or assets are locked in a smart contract, they cannot be transferred or used until the lock-up period has expired or certain conditions have been met.

Contract owner can lock the user funds

✗ The owner is able to lock the contract

Description	Locking the contract means that the owner is able to lock any funds of addresses that they are not able to transfer bought tokens anymore.
Example	An example of locking is by pausing the contract. That causes that the users is not able to transfer claim anymore.
Comment	The owner can pause all the functionalities of the contracts

Alleviation - As a safety, if something goes wrong, eg. missed vesting percentage, token amount, etc.

External/Public functions

External/public functions are functions that can be called from outside of a contract, i.e., they can be accessed by other contracts or external accounts on the blockchain. These functions are specified using the function declaration's external or public visibility modifier.

State variables

State variables are variables that are stored on the blockchain as part of the contract's state. They are declared at the contract level and can be accessed and modified by any function within the contract. State variables can be defined with a visibility modifier, such as public, private, or internal, which determines the access level of the variable.

Components

 Contracts	 Libraries	 Interfaces	 Abstract
7	0	6	0


Exposed Functions

This section lists functions that are explicitly declared public or payable. Please note that getter methods for public stateVars are not included.

 Public	 Payable
92	0





External	Internal	Private	Pure	View
76	110	0	0	32

StateVariables

Total	 Public
45	40



Capabilities

Solidity Versions observed	 Experimental Features	 Can Receive Funds	 Uses Assembly	 Has Destroyable Contracts
<code>^0.8.19</code> <code>^0.8.0</code>			yes	





Centralization Privileges

Centralization can arise when one or more parties have privileged access or control over the contract's functionality, data, or decision-making. This can occur, for example, if a single entity controls the contract or if certain participants have special permissions or abilities that others do not.

In the project, some authorities have access to the following functions:

File	Privileges
FixedVestingV2	<ul style="list-style-type: none"> • only Factory Owner <ul style="list-style-type: none"> • Insert New Vestings • Update Vesting Date Time to an arbitrary value • Update Vesting Ratio in percent • Manually Remove last vesting round • Manually Insert New buyer addresses and their purchase in the vesting • Replace buyer addresses for a new purchase • Replace Purchases for new buyers • Remove buyers from vesting • Withdraw all tokens from the contract's balance at any time • Set token price to an arbitrary value • Set/Update Vesting token and Stable coin address • Set the time of last refund • Set/Update Project Owner address • Pause/Unpause the functionalities of the contract

File	Privileges
LinearVestingV2	<ul style="list-style-type: none"> • only Factory Owner <ul style="list-style-type: none"> • Update Vesting Date Time to an arbitrary value • Update TGE Ratio in percent • Manually Insert New buyer addresses and their purchase in the vesting • Replace buyer addresses for a new purchase • Replace Purchases for new buyers • Remove buyers from vesting • Withdraw all tokens from the contract's balance at any time • Set token price to an arbitrary value • Set/Update Vesting token and Stable coin address • Set the time of last refund • Set/Update Project Owner address • Pause/Unpause the functionalities of the contract
Refunder	<ul style="list-style-type: none"> • only Factory Owner <ul style="list-style-type: none"> • Refund tokens to users • Withdraw all tokens from the contract's balance at any time • Set Stable and Project Owner address • Set/Change the date time when the project owner could claim their stable • Pause/Unpause Vesting Activity

Recommendations

To avoid potential hacking risks, it is advisable for the client to manage the private key of the privileged account with care. Additionally, we recommend enhancing the security practices of centralized privileges or roles in the protocol through a decentralized mechanism or smart-contract-based accounts, such as multi-signature wallets.

Here are some suggestions of what the client can do:

- Consider using multi-signature wallets: Multi-signature wallets require multiple parties to sign off on a transaction before it can be executed, providing an extra layer of security e.g. Gnosis Safe
- Use of a timelock at least with a latency of e.g. 48-72 hours for awareness of privileged operations
- Introduce a DAO/Governance/Voting module to increase transparency and user involvement



- Consider Renouncing the ownership so that the owner can no longer modify any state variables of the contract. Make sure to set up everything before renouncing.





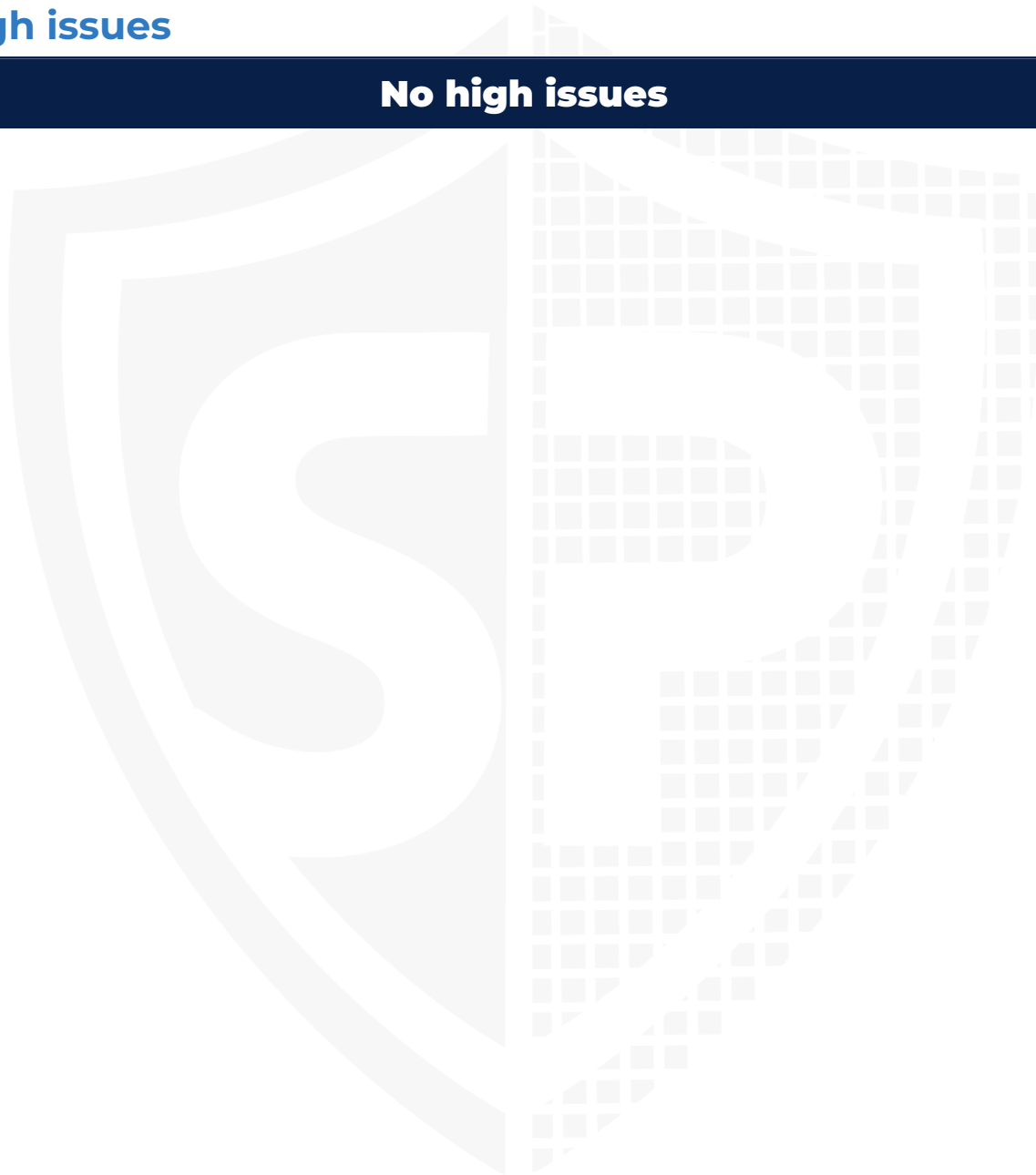
Audit Results

Critical issues

No critical issues

High issues

No high issues



Medium issues

#1 | Owner can Lock Contracts

File	Severity	Location	Status
All	Medium	N/A	ACK

Description - The contracts implement pausing functionality, allowing the owner to lock all the contracts at their discretion. Thus, when the contract is paused, no functionality will be active.

Remediation - We recommend not to pause the claim functionality.

Alleviation - As a safety, if something goes wrong, eg. missed vesting percentage, token amount, etc.

#2 | Owner can drain tokens

File	Severity	Location	Status
FixedVestingV2	Medium	L520	ACK
LinearVestingV2	Medium	L503	ACK
Refunder	Medium	L153	ACK

Description - The contract owner can drain the contract's complete balance by calling this function.

Remediation - Make sure that it is not possible to take out vested tokens.

Alleviation - As a safety, if something goes wrong, eg. missed vesting percentage, token amount, etc.

Low issues

#1 | Missing Events

File	Severity	Location	Status
FixedVestingV2	Low	L243—383, L535—568	ACK

Description - Make sure to emit events for all the critical parameter changes in the contract to ensure the transparency and trackability of all the state variable changes.

#2 | Logical Error

File	Severity	Location	Status
FixedVestingV2	Low	L252	ACK

Description - The function does not have a check to verify that the time of the vesting must be set in the future.

#3 | Missng “isContract” check

File	Severity	Location	Status
FixedVestingV2	Low	L543, 559	ACK
LinearVestingV2	Low	L526, 542	ACK

Description - The contract has no checks to verify whether an EOA or contract is being set.

Remediation - We recommend putting in a check to verify that the address must be a contract.

Informational issues

#1 | Disable initializing

File	Severity	Location	Status
All	Informational	N/A	ACK

Description - If the owner updates the contract, a disableInitializer call in the constructor must be implemented. This prevents calling the initialize function again to set the state variables in the contract. This should be implemented only if the contract was deployed before. Otherwise, the owner cannot call the initialize function to set the variables.

Recommendation - If the contract hasn't been deployed, remove the disableInitializer in the constructor. Otherwise, you are not able to initialize the contract. When the contract has a deployed version already, leave it as it is.

#2 | Floating Pragma

File	Severity	Location	Status
All	Informational	N/A	ACK

Description - The contracts should be deployed with the same compiler version and flag that they have been tested thoroughly. Locking the pragma helps to ensure that contracts do not accidentally get deployed using other versions.

Legend for the Issue Status

Attribute or Symbol	Meaning
Open	The issue is not fixed by the project team.
Fixed	The issue is fixed by the project team.
Acknowledged(ACK)	The issue has been acknowledged or declared as part of business logic.



**Blockchain Security | Smart Contract Audits | KYC
Development | Marketing**

MADE IN GERMANY