



SOLIDProof

Bring trust into your projects

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

MADE IN GERMANY

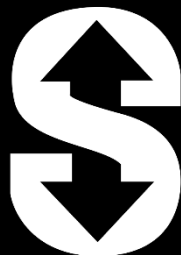
Swirl Protocol

AUDIT

SECURITY ASSESSMENT

01. August, 2023

FOR



SolidProof_io



@solidproof_io



Introduction	3
Disclaimer	3
Project Overview	4
Summary	4
Social Medias	4
Audit Summary	5
File Overview	6
Imported packages	6
Components	7
Exposed Functions	7
Capabilities	8
Inheritance Graph	9
Audit Information	10
Vulnerability & Risk Level	10
Auditing Strategy and Techniques Applied	11
Methodology	11
Overall Security	12
Upgradeability	12
Ownership	13
Ownership Privileges	14
Minting tokens	14
Burning tokens	15
Blacklist addresses	16
Fees and Tax	17
Lock User Funds	18
Centralization Privileges	19
Audit Results	20

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	Swirl Protocol
Website	https://www.swirlend.com/
About the project	Swirl Protocol is an EVM compatible lending/borrowing protocol that launched on Linea Network. Swirl Lending provides peer-to-peer lending solutions that are fully decentralized, transparent and non-custodial. Similar to (and based from) existing lending platforms like Compound Finance and AAVE users will be able to lend any supported assets on our platform, and use their capital to borrow supported assets.
Chain	Linea
Language	Solidity
Codebase	https://github.com/SwirlLend/compound-8.10/tree/main
Commit	N/A
Unit Tests	Not Provided

Social Medias

Telegram	https://t.me/swirlnews
Twitter	https://twitter.com/SwirlLend
Facebook	N/A
Instagram	N/A
GitHub	https://github.com/SwirlLend
Reddit	N/A
Medium	N/A
Discord	https://discord.com/invite/MkzKEZF2Fx
YouTube	N/A
TikTok	N/A
LinkedIn	N/A

Audit Summary

Version	Delivery Date	Change Log
v1.0	29. July 2023	<ul style="list-style-type: none"> · Layout Project · Automated/ Manual-Security Testing · Summary
v1.1	01. August 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. 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 it was not functionally tested by us. This project is 1:1 fork with compound, All the contracts with comments are same as compound. Also, the project contains some of the low issues as compound protocol and we will treat them as acknowledged since the code is same.



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/CTokenInterfaces.sol	3b4585ce0c88d1d769a7187da2f0ef4290d2c962
contracts/CEther.sol	c6a001e27e3ac5ab29dff25a73fc78ac34ae7c47
contracts/ChainLinkOracle.sol	f394c8c4304721777efe3e8ae485851a3a899607
contracts/Governance/Comp.sol	6253b336d0f0df5f9751059f0cedcb265a096401
contracts/JumpRateModelV4.sol	4d9b456ba3a50ce534cb93ef93f50ba33f476a9f
contracts/Ownership/Ownable.sol	efc2370a491896b3501410d70fcdd29f02beb4e4
contracts/ComptrollerStorage.sol	1a2e4f07d7a0d6ea794db122ba5c0de9689bde6e
contracts/InterestRateModel.sol	dcb0c8ac69fdc0008b495c71d09ba8fb8c09d819
contracts/EIP20Interface.sol	bd556fa88dd92c232691362bfff7f565887cb48
contracts/Unitroller.sol	2a679a953422ce85ad1135663ea1a3d4a72d484a
contracts/ErrorReporter.sol	95e30d4e8fce1e5a804c15b844928540e740e16d
contracts/SafeMath.sol	04f62f48e9092c08e5af35b57db369c05c20faf7
contracts/ExponentialNoError.sol	f57f0095268ddf489e8a39ae6d00842f60831115
contracts/CToken.sol	a4a1c30a8a32b5574528dfe194bab01f4f4e67d8
contracts/PriceOracle.sol	25f671851dede71fe4910c069b47d206e9f53d39



File Name	SHA-1 Hash
contracts/CErc20.sol	81dfc9b4f5d53990a45c30cf52742a9acec5f2d d
contracts/Comptroller.sol	0ad62e0551b25a336ed67f5541e25b4ee2f043a 6
contracts/BasePriceOracle.sol	ee23dc2bbc62725e1b87e82056e896bd900a6 b35
contracts/ComptrollerInterface.sol	e2b225fe47d4fc5e108e8cc0321308010b16f66 b
contracts/EIP20NonStandardInterf ace.sol	e2435b5dde51e630flab2b6ece09e63e00e6f8 a5

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) be an indication of a changed state or potential vulnerability that was not the subject of this scan.

Imported packages

Used code from other Frameworks/Smart Contracts.

N/A

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





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 needed within visibility modifier, such as public, private or internal, which determines the access level of the variable.

Components

 Contracts	 Libraries	 Interfaces	 Abstract
22	1	4	9


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
193	7





External	Internal	Private	Pure	View
146	281	0	46	63






StateVariables

Total	 Public
91	73



Capabilities

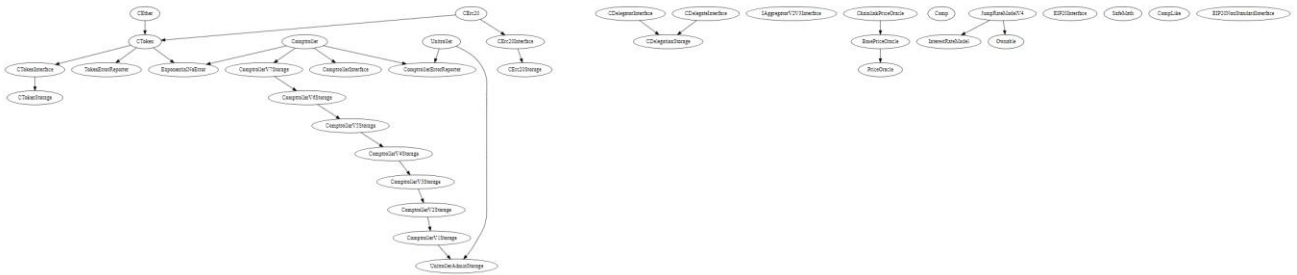
Solidity Versions observed	 Experimental Features	 Can Receive Funds	 Uses Assembly	 Has Destroyable Contracts
<code>^0.8.10</code>	<code>-----</code>	<code>yes</code>	<code>yes</code> <code>(4 asm</code> <code>blocks)</code>	<code>-----</code>

 Transfers ETH	 Low-Level Calls	 DelegateCall	 Uses Hash Functions	 ECRrecover	 New/Create/Create2
<code>yes</code>		<code>yes</code>	<code>yes</code>	<code>yes</code>	

 TryCatch	Σ Unchecked
	<code>yes</code>

Inheritance Graph

An inheritance graph is a graphical representation of the inheritance hierarchy among contracts. In object-oriented programming, inheritance is a mechanism that allows one class (or contract, in the case of Solidity) to inherit properties and methods from another class. It shows the relationships between different contracts and how they are related to each other through inheritance.



Audit Information

Vulnerability & Risk Level

Risk represents the probability that a certain source threat will exploit the 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 not an upgradable



Deployer cannot update the contract with new functionalities.

Description	The contract is not an upgradeable contract. The Deployer is not able to change or add any functionalities to the contract after deploying.
Comment	N/A



Ownership

The ownership is not renounced

✗ The ownership is not renounced

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.

Example	N/A
Comment	N/A

Note – *The contract cannot be considered as renounced till it is not deployed or having some functionality that can change the state of the contract.*



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	Owner cannot mint new tokens manually.
Comment	It is a lending protocol. cToken can't be minted manually. When a user mints, redeems, borrows, repays a borrow, liquidates a borrow, or transfers cTokens, she will do so using the cToken contract.



Burning tokens

Burning tokens is the process of 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 set fees more than 25%

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 token 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 cannot lock user funds.



The owner cannot lock user funds

Description

The owner is not able to lock the contract by any functions or updating any variables.

Comment

N/A

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 the contract is controlled by a single entity or if certain participants have special permissions or abilities that others do not.

In the project, there are authorities that have access to the following functions:

File	Privileges
BasePriceOracle.sol	➤ The provider can set a new provider address.
JumpRateModelV4.sol	➤ The owner can update the jump rate model. ➤ The owner can set any number to blocks per year.

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 cannot modify any state variables of the contract anymore. Make sure to set up everything before renouncing.

Audit Result

#1 | Dangerous minting functionality

File	Severity	Location	Status
CEther.sol	Medium	L309-330	ACK

Description - Anyone can mint tokens if the mintGuardianPaused is set to false. Also, If the cToken address is listed. It is recommended that the caller can only be cToken so that no one will be able to manipulate the updateCompSupply. Also, Compound does not use this functionality so we would recommend removing the function that can manipulate the contract in a terrible way.

Alleviation - It is a lending protocol. cToken can't be minted manually. When a user mints, redeems, borrows, repays a borrow, liquidates a borrow, or transfers cTokens, she will do so using the cToken contract.

#2 | Floating pragma solidity version

File	Severity	Location	Status
All	Low	--	ACK

Description - It is recommended to add the constant version of solidity as this prevents the unintentional deployment of a contract with an outdated compiler that contains unresolved bugs.

#3 | Missing Zero Address Validation

File	Severity	Location	Status
BasePriceOracle.sol	Low	L15	ACK

Description - Check that the address is not zero.

Remediation - Add a 'require' check to avoid these circumstances.

#4 | Missing Events Arithmetic

File	Severity	Location	Status
BasePriceOracle.sol	Low	L15-17	ACK
CToken.sol	Low	L1092	ACK
CERC20.sol	Low	L26	ACK

Description - Emit an event for critical parameter changes.

#5 | Function that are not used

File	Severity	Location	Status
BasePriceOracle.sol	Informational	L19-27	ACK
ErrorReporter.sol	Informational	L58-62	ACK
ExponentialNoError.sol	Informational	L60-162	ACK

Description- Remove unused functions.

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