DeHacker

Code Security Assessment

Sorta Finance

July 12th, 2024

Contents

Summary

DeHacker's objective was to evaluate the repository for security-related issues, code quality, and adherence to specification and best practices.
Possible issues we looked for included (but are not limited to):

- Transaction-ordering dependence
- Timestamp dependence
- Mishandled exceptions and call stack limits
- Unsafe external calls
- Integer overflow/underflow
- Number rounding errors
- Reentrancy and cross-function vulnerabilities
- Denial of service/logical oversights
- Access control
- Centralization of power
- Business logic contradicting the specification
- Code clones, functionality duplication
- Gas usage
- Arbitrary token minting

Issue Categories

Every issue in this report was assigned a severity level from the following:

Critical severity issues

A vulnerability that can disrupt the contract functioning in a number of scenarios or creates a risk that the contract may be broken.

Major severity issues

A vulnerability that affects the desired outcome when using a contract or provides the opportunity to use a contract in an unintended way.

Medium severity issues

A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.

Minor severity issues

A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.

Informational

A vulnerability that has informational character but is not affecting any of the code.

Overview

Project Summary

Project Name	Sorta Finance
Platform	Arbitrum
website	https://www.sorta.finance/
Type	DeFi
Language	Solidity
Codebase	https://github.com/SortaFi/Sorta-Finance

Vulnerability Summary

Vulnerability Level	Total	Pending	Declined	Acknowledged	Partially Resolved	Resolved
Critical	0	0	0	0	0	0
Major	1	0	0	0	0	1
Medium	0	0	0	0	0	0
Minor	4	0	0	4	0	0
Informational	1	0	0	1	0	0
Discussion	0	0	0	0	0	0

Audit scope

ID	File	SHA256 Checksum
DKE	https://github.com/SortaFi/Sorta-Finance	f4cbb40e314d20344ca27ae875d06f3415cc6ae7d9913473ce2745011fe792ce

Findings

ID	Issue	Severity	Status
Global-01	Centralization Related Risks	Major	Resolved
EDO-01	Parameter Modifiers	Minor	Acknowledged
EDO-02	Uninitialized State Variables	Minor	Acknowledged
EDO-03	Optimize Gas	Minor	Acknowledged
DKE-01	Unchecked Transfer	Minor	Acknowledged
DKE-02	Missing zero address validation	Informational	Acknowledged

MAJOR

GLOBAL-01 | Centralization Related Risks

Issue	Severity	Location	Status
Centralization Related Risks	Major	Global	Resolved

Description

The owner of the Comptroller contract has the following permissions:
- function _setRewardDistributor()
- function _setPriceOracle()
- function _setCloseFactor()
- function _setCollateralFactor()
- function _setLiquidationIncentive()
- function _supportMarket()
- function _setMarketBorrowCaps()
- function _setBorrowCapGuardian()
- function _setPauseGuardian()
- function _setMintPaused()
- function _setBorrowPaused()
- function _setTransferPaused()
- function _setSeizePaused()

The owner will have the ability to influence the operation results of the protocol.

Recommendation

This finding describes the level of decentralization of the project, and it is recommended to strengthen security and improve the degree of decentralization from the following aspects:

- It is recommended that privileged addresses use multi-signature wallet addresses.
- For modification operations that affect protocol operation stability and key business parameters, it is recommended to implement time locks.

MINOR

EDO-01 | Function Visibility Optimization

Issue	Severity	Location	Status
Comptroller.sol #1	Minor	Line 123	Acknowledged

Description

```solidity
function enterMarkets(address[] memory cTokens) external returns (uint[] memory) {
    uint len = cTokens.length;

    uint[] memory results = new uint[](len);
    for (uint i = 0; i < len; i++) {
        CToken cToken = CToken(cTokens[i]);

        results[i] = uint(addToMarketInternal(cToken, msg.sender));
    }

    return results;
}
```

Data location must be "calldata" for parameter in external function, but "memory" was given.

Recommendation

Use "calldata" instead of "memory".

MINOR

EDO-02 | Uninitialized State Variables

Issue	Severity	Location	Status
Comptroller.sol #2	Minor	Line 1120	Acknowledged

Description

```solidity
function adminOrInitializing() internal view returns (bool) {
    return msg.sender == admin || msg.sender == comptrollerImplementation;
}
```

The comptrollerImplementation variable is not initialized.

Recommendation

If necessary, it is recommended to initialize it.

MINOR

EDO-03 | Optimize Gas

Issue	Severity	Location	Status
Comptroller.sol #3	Minor	Line 982	Acknowledged

Description

```solidity
function _addMarketInternal(address cToken) internal {
    for (uint i = 0; i < allMarkets.length; i ++) {
        require(allMarkets[i] != CToken(cToken), "market already added");
    }
    allMarkets.push(CToken(cToken));
}
```

Loop condition should use cached array length instead of referencing length member of the storage array.

Recommendation

Cache the lengths of storage arrays to optimize gas.

MINOR

DKE-01 | Unchecked Transfer

Issue	Severity	Location	Status
RewardDistributor.sol #1	Minor	Line 407	Acknowledged

Description

```solidity
function grantRewardInternal(uint8 rewardType, address payable user, uint256 amount
) internal returns (uint256) {
    address rewardAddress = rewardAddresses[rewardType];
    EIP20Interface reward = EIP20Interface(rewardAddress);
    uint256 rewardRemaining = reward.balanceOf(address(this));
    if (amount > 0 && amount <= rewardRemaining) {
        reward.transfer(user, amount);
        return 0;
    }

    return amount;
}
```

The return value of an external transfer call is not checked.

Recommendation

It is recommended to use SafeERC20.

INFORMATIONAL

DKE-02 | Missing zero address validation

Issue	Severity	Location	Status
RewardDistributor.sol #2	Informational	Line 476	Acknowledged

Description

```solidity
function setAdmin(address _newAdmin) public {
    require(msg.sender == admin, "only admin can set admin");
    admin = _newAdmin;
}
```

There is no non-zero check for the admin parameter. Incorrect settings may lead to some unexpected consequences.

Recommendation

It is recommended to perform a non-zero check.

Disclaimer

This report is based on the scope of materials and documentation provided for a limited review at the time provided. Results may not be complete nor inclusive of all vulnerabilities. The review and this report are provided on an as-is, where-is, and as-available basis. You agree that your access and/or use, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your sole risk. Blockchain technology remains under development and is subject to unknown risks and flaws. The review does not extend to the compiler layer, or any other areas beyond the programming language, or other programming aspects that could present security risks. A report does not indicate the endorsement of any particular project or team, nor guarantee its security. No third party should rely on the reports in any way, including for the purpose of making any decisions to buy or sell a product, service or any other asset. To the fullest extent permitted by law, we disclaim all warranties, expressed or implied, in connection with this report, its content, and the related services and products and your use thereof, including, without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. We do not warrant, endorse, guarantee, or assume responsibility for any product or service advertised or offered by a third party through the product, any open source or third-party software, code, libraries, materials, or information linked to, called by, referenced by or accessible through the report, its content, and the related services and products, any hyperlinked websites, any websites or mobile applications appearing on any advertising, and we will not be a party to or in any way be responsible for monitoring any transaction between you and any third-party providers of products or services. As with the purchase or use of a product or service through any medium or in any environment, you should use your best judgment and exercise caution where appropriate.

FOR AVOIDANCE OF DOUBT, THE REPORT, ITS CONTENT, ACCESS, AND/OR USAGE THEREOF, INCLUDING ANY ASSOCIATED SERVICES OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, INVESTMENT, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

Appendix

Finding Categories

Centralization / Privilege

Centralization / Privilege findings refer to either feature logic or implementation of components that act against the nature of decentralization, such as explicit ownership or specialized access roles in combination with a mechanism to relocate funds.

Coding Style

Coding Style findings usually do not affect the generated bytecode but rather comment on how to make the codebase more legible and, as a result, easily maintainable.

Volatile Code

Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that may result in a vulnerability.

Logical Issue

Logical Issue findings detail a fault in the logic of the linked code, such as an incorrect notion on how block. timestamp works.

Checksum Calculation Method

The "Checksum" field in the "Audit Scope" section is calculated as the SHA-256 (Secure Hash Algorithm 2 with digest size of 256 bits) digest of the content of each file hosted in the listed source repository under the specified commit.

The result is hexadecimal encoded and is the same as the output of the Linux “sha256sum" command against the target file.

About

DeHacker is a team of auditors and white hat hackers who perform security audits and assessments. With decades of experience in security and distributed systems, our experts focus on the ins and outs of system security. Our services follow clear and prudent industry standards. Whether it's reviewing the smallest modifications or a new platform, we'll provide an in-depth security survey at every stage of your company's project. We provide comprehensive vulnerability reports and identify structural inefficiencies in smart contract code, combining high-end security research with a real-world attacker mindset to reduce risk and harden code.

BLOCKCHAIINS

- Ethereum
- Cosmos
- Eos
- Substrate

TECH STACK

- Python
- Solidity
- Rust
- c++

CONTACTS

- https://dehacker.io
- https://twitter.com/dehackerio
- https://github.com/dehacker/audits_public
- https://t.me/dehackerio
- https://blog.dehacker.io/

DeHacker

July 2024