OBToken Smart Contract
Audit Report - October 2021

Submitted By

Antier Solutions

Contents

Disclaimer

This is a limited audit report based on our analysis of the OBToken Smart Contract. It covers industry best practices as of the date of this report, concerning: smart contract best coding practices, cybersecurity vulnerabilities, issues in the framework and algorithms based on white paper, code, the details of which are set out in this report, (Source Code); the Source Code compilation, deployment, and functionality (performing the intended functions).

Smart contracts are deployed and executed on the blockchain. The platform, its programming language, and other software related to the smart contract can have vulnerabilities that can lead to hacks.

You are advised to read the full report to get a full view of our analysis. While we did our best in producing this report, it is important to note that you should not rely on this report, and cannot claim against us, based on what it says or does not say, or how we produced it, and you need to conduct your independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

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 all copies of this report downloaded and/or printed by you.

The report is provided "as is," without any condition, warranty, or other terms of any kind except as set out in this disclaimer. TAS 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 affect the report.

Executive Summary

OBToken commissioned Antier Solutions to perform an end-to-end source code review of their Solidity Smart Contract. Team Antier Solutions (referred to as TAS throughout the report) performed the audit from October 6, 2021, to October 8, 2021.

The following report discusses severity issues and their scope of rectification through change recommendations. It also highlights activities that are successfully executed and others that need total reworking (if any).

The report emphasizes best practices in coding and the security vulnerabilities if any.

The information in this report should be used to understand the overall code quality, security, and correctness of the Smart Contract. The analysis is static and entirely limited to the Smart Contract code.

In the audit, we reviewed the Smart Contract's code that implements the token mechanism.

Scope

We performed an independent technical audit to identify Smart Contract uncertainties. This shall protect the code from illegitimate authorization attempts or external & internal threats of any type. This also ensures end-to-end proofing of the contract from frauds.

The audit was performed semi-manually. We analyzed the Smart Contract code line-by-line and used an automation tool to report any suspicious code.

We considered the following standards for the Smart Contract code review:

- ERC20 [Token Contract best practices]

We used the following tools to perform automated tests:

- Ethereum Development platform:
  Hardhat
- Framework :
  Remix Ethereum
- Automation tools:
  - Slither
  - Surya
  - Mythril

Audit Goals

The focus of the audit was to verify that the Smart Contract system was secure, resilient, and worked according to the specifications provided to the Auditing team.

TAS grouped the audit activities in the following three categories:

- **Security**
  Identifying security-related issues within each contract and the system of contracts

- **Architecture**
  Evaluation of the system architecture against smart contract conventions and general software best practices

- **Code Correctness and Quality**
  A full review of the contract source code. The primary areas of focus include:
  - Correctness
  - Readability
  - Sections of code with high complexity
  - Quantity and quality of test coverage

Result

The audit was conducted on the single contract file provided to the Auditing team. The following table provides an overall picture of the security posture. ✔ means no bugs were identified.

#	SMART CONTRACT PENETRATION TEST (OBJECTIVES)	AUDIT SUBCLASS	RESULT
1	OVERFLOW	-	✓
2	RACE CONDITION	-	✓
3	PERMISSIONS	-	✓
4	SAFETY DESIGN	OpenZeppelin safemath	✓
5	DDOS ATTACK	Call function security	✓
OVERALL SECURITY POSTURE		**Secure**	

Recommendations

The OBToken development team demonstrated high technical capabilities, both in the design of the token and implementation of the Smart Contract. Overall, the code includes effective use of abstraction, separation of concerns, and modularity.

Code Quality and Readability

The code follows all coding conventions, no missing patterns, or corner cases. The comments should be provided for each functionality to enhance the readability quotient.

```
ftrace | funcSig
function addVestingScheme(uint256[] calldata vestingamounts ) public onlyOwner returns (uint) {
    _maxvestingid += 1;
    _vestingschedules[_maxvestingid] = vestingamounts ;
    return _maxvestingid;
}

ftrace | funcSig
function addVestingAddress(address addr , uint vestingid ) public onlyOwner {
    require(_vestingaddresses[addr ] == 0, "Cannot change vesting schedule after it's set");
    _vestingaddresses[addr ] = vestingid ;
}

ftrace | funcSig
function vestingRequirements(address addr ) public view returns (uint256[] memory) {
    uint vestid = _vestingaddresses[addr ];
    return _vestingschedules[vestid];
}
```

Function's comments should include @dev, @notice, @param for total compliance with Solidity standards.

Code security

TAS performed a static analysis of the code to identify possible loopholes. This verified whether the contract adhered to the Solidity best practices.

Implementation instructions

Include Unit Test cases for better understanding and testing of Gas limits. All the implementation instructions should be written in the README file.

Severity Level References

The following severity levels will describe the degree of every issue:

High severity issues

The issue puts the majority of, or large numbers of, users' sensitive information at risk, or is reasonably likely to lead to a catastrophic impact on the client's reputation or serious financial implications for the client and users.

Medium severity issues

The issue puts a subset of individual users' sensitive information at risk; exploitation would be detrimental to the client's reputation or is reasonably likely to lead to moderate financial impact.

Low severity issues

The risk is relatively low and could not be exploited regularly, or it's a risk not indicated as important or impactful by the client because of the client's business circumstances.

Informational

The issue does not pose an immediate threat to continued operation or usage but is relevant for security best practices, software engineering best practices, or defensive redundancy.

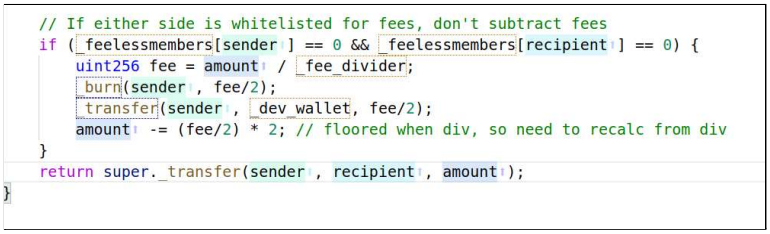
Optimization issue

The issue does not pose an immediate threat to continued operation or usage but is relevant for code optimization and gas efficiency best practices.

Number of vulnerabilities per severity

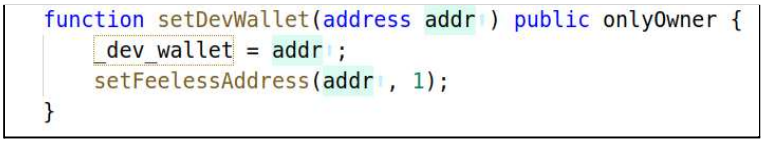
High	Medium	Low	Informational
0	2	2	2

Medium Severity Vulnerabilities

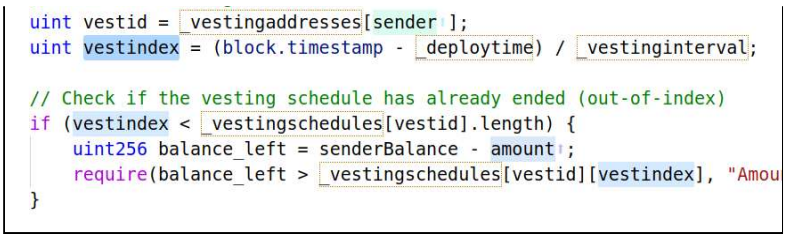
Severity	**Medium**
Contract	**OBToken**
Description	**Use Safe Math**
Code	You have imported SafeMath, but never used it.  ``` // If either side is whitelisted for fees, don't subtract fees if (_feelessmembers[sender] == 0 && _feelessmembers[recipient] == 0) { uint256 fee = amount / _fee_divider; _burn(sender, fee/2); _transfer(sender, _dev_wallet, fee/2); amount -= (fee/2) * 2; // floored when div, so need to recalc from div } return super._transfer(sender, recipient, amount); } ```
Recommendation	Arithmetic operations in Solidity wrap on overflow. This can easily result in bugs because programmers usually assume that an overflow raises an error, which is the standard behavior in high-level programming languages. SafeMath restores this intuition by reverting the transaction when an operation overflows.
Status	**Fixed**

Severity	**Medium**
Contract	**OBToken**
Description	**Divide before multiplication**
Code	`amount -= (fee/2) * 2;`
Recommendation	Solidity integer division might truncate. As a result, performing multiplication before division can sometimes avoid loss of precision.
Status	**Acknowledged (For having a Floored value)**

Low Severity Vulnerabilities

Severity	Low
Contract	**OBToken**
Description	**Lack of zero-check**
Code	
Recommendation	Add missing zero address validation.
Status	**Acknowledged (Client suggested they have intentionally left this un-checked, as they may want to burn the tokens going to _dev_wallet)**

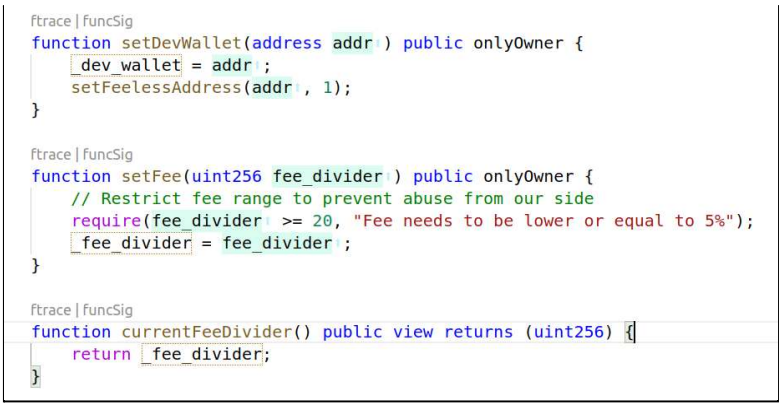
```
function setDevWallet(address addr) public onlyOwner {
    _dev_wallet = addr;
    setFeelessAddress(addr, 1);
}
```

Severity	Low
Contract	OBToken
Description	Uses timestamp for comparisons
Code	
Recommendation	Dangerous usage of block.timestamp. block.timestamp can be manipulated by miners.
Status	Acknowledged (Client suggested they are using longer timeframes).

```
uint vestid = _vestingaddresses[sender];
uint vestindex = (block.timestamp - _deploytime) / _vestinginterval;

// Check if the vesting schedule has already ended (out-of-index)
if (vestindex < _vestingschedules[vestid].length) {
    uint256 balance_left = senderBalance - amount;
    require(balance_left > _vestingschedules[vestid][vestindex], "Amou
}
```

Informational Severity Vulnerabilities

Severity	Informational
Contract	**OBToken**
Recommendation	**A public function that could be declared external**
Code	
Description	Gas can be optimized to avoid over-public declaration.
Status	**Fixed**

Severity	Informational
Contract	**OBToken**
Recommendation	**Imported ERC20 twice**
Code	`6 import "@openzeppelin/contracts/token/ERC20/ERC20.sol";` `7 import "@openzeppelin/contracts/token/ERC20/extensions/ERC20Burnable.sol";`
Description	ERC20Burnable is an extension of ERC20. Therefore, ERC20Burnable already inherited ERC20, so we don't need to import it again.
Status	**Fixed**

Technical Analysis

The following is our automated and manual analysis of the Talarity Smart Contract code:

Checked Vulnerabilities

We checked Talarity Smart Contract for commonly known and specific business logic vulnerabilities. Following is the list of vulnerabilities tested in the Smart Contract code:

- Reentrancy
- Timestamp Dependence
- Gas limit and loops
- DoS with (unexpected) throw
- DoS with (unexpected) revert
- DoS with block gas limit
- Transaction-ordering dependence
- Use of tx.origin
- Exception disorder
- Gasless send
- Balance equality
- Byte array
- Transfer forwards all gas
- ERC20 API violation

- Malicious libraries
- Compiler version not fixed
- Redundant fallback function
- Send instead of transfer
- Style guide violation
- Unchecked external call
- Unchecked math
- Unsafe type inference
- Implicit visibility level
- Address hardcoded
- Using delete for arrays
- Integer overflow/underflow
- Locked money
- Private modifier
- Revert/require functions
- Using var
- Visibility

Automation Report

TAS used Slither and Mythril to generate the automation report.

Slither

Slither is a Solidity static analysis framework written in Python 3. It runs a suite of vulnerability detectors, prints visual information about contract details, and provides an API to write custom analyses. Slither enables developers to find vulnerabilities, enhance their code comprehension, and quickly prototype custom analyses.

```
INFO:Printers:
Compiled with Builder
Number of lines: 97 (+ 825 in dependencies, + 0 in tests)
Number of assembly lines: 0
Number of contracts: 1 (+ 7 in dependencies, + 0 tests)

Number of optimization issues: 19
Number of informational issues: 12
Number of low issues: 2
Number of medium issues: 1
Number of high issues: 0


Use: Openzeppelin-Ownable, Openzeppelin-ERC20, Openzeppelin-SafeMath
ERCs: ERC20

+---------+-------------+-------+--------------------+--------------+----------+
|   Name  | # functions |  ERCS |     ERC20 info     | Complex code | Features |
+---------+-------------+-------+--------------------+--------------+----------+
| OBToken |      45     | ERC20 |     No Minting     |      No      |          |
|         |             |       | Approve Race Cond. |              |          |
|         |             |       |                    |              |          |
+---------+-------------+-------+--------------------+--------------+----------+
INFO:Slither:. analyzed (8 contracts)
INFO:Slither:Use https://crytic.io/ to get access to additional detectors and Github integration
```

```
burn(uint256) should be declared external:
        - ERC20Burnable.burn(uint256) (node_modules/@openzeppelin/contracts/token/ERC20/extensions/ERC20Burnable
.sol#19-21)
burnFrom(address,uint256) should be declared external:
        - ERC20Burnable.burnFrom(address,uint256) (node_modules/@openzeppelin/contracts/token/ERC20/extensions/E
RC20Burnable.sol#34-41)
setDevWallet(address) should be declared external:
        - OBToken.setDevWallet(address) (contracts/token.sol#33-36)
setFee(uint256) should be declared external:
        - OBToken.setFee(uint256) (contracts/token.sol#38-42)
currentFeeDivider() should be declared external:
        - OBToken.currentFeeDivider() (contracts/token.sol#44-46)
addVestingScheme(uint256[]) should be declared external:
        - OBToken.addVestingScheme(uint256[]) (contracts/token.sol#52-56)
addVestingAddress(address,uint256) should be declared external:
        - OBToken.addVestingAddress(address,uint256) (contracts/token.sol#58-61)
vestingRequirements(address) should be declared external:
        - OBToken.vestingRequirements(address) (contracts/token.sol#63-66)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-
external
INFO:Slither:. analyzed (8 contracts with 75 detectors), 34 result(s) found
```

```
INFO:Detectors:
renounceOwnership() should be declared external:
        - Ownable.renounceOwnership() (node_modules/@openzeppelin/contracts/access/Ownable.sol#53-55)
transferOwnership(address) should be declared external:
        - Ownable.transferOwnership(address) (node_modules/@openzeppelin/contracts/access/Ownable.sol#61-64)
name() should be declared external:
        - ERC20.name() (node_modules/@openzeppelin/contracts/token/ERC20/ERC20.sol#61-63)
symbol() should be declared external:
        - ERC20.symbol() (node_modules/@openzeppelin/contracts/token/ERC20/ERC20.sol#69-71)
decimals() should be declared external:
        - ERC20.decimals() (node_modules/@openzeppelin/contracts/token/ERC20/ERC20.sol#86-88)
totalSupply() should be declared external:
        - ERC20.totalSupply() (node_modules/@openzeppelin/contracts/token/ERC20/ERC20.sol#93-95)
transfer(address,uint256) should be declared external:
        - ERC20.transfer(address,uint256) (node_modules/@openzeppelin/contracts/token/ERC20/ERC20.sol#112-115)
approve(address,uint256) should be declared external:
        - ERC20.approve(address,uint256) (node_modules/@openzeppelin/contracts/token/ERC20/ERC20.sol#131-134)
transferFrom(address,address,uint256) should be declared external:
        - ERC20.transferFrom(address,address,uint256) (node_modules/@openzeppelin/contracts/token/ERC20/ERC20.so
l#149-163)
increaseAllowance(address,uint256) should be declared external:
        - ERC20.increaseAllowance(address,uint256) (node_modules/@openzeppelin/contracts/token/ERC20/ERC20.sol#1
77-180)
decreaseAllowance(address,uint256) should be declared external:
        - ERC20.decreaseAllowance(address,uint256) (node_modules/@openzeppelin/contracts/token/ERC20/ERC20.sol#1
96-204)
```

```
INFO:Detectors:
Pragma version^0.8.0 (node_modules/@openzeppelin/contracts/access/Ownable.sol#3) necessitates a version too rece
nt to be trusted. Consider deploying with 0.6.12/0.7.6
Pragma version^0.8.0 (node_modules/@openzeppelin/contracts/token/ERC20/ERC20.sol#3) necessitates a version too r
ecent to be trusted. Consider deploying with 0.6.12/0.7.6
Pragma version^0.8.0 (node_modules/@openzeppelin/contracts/token/ERC20/IERC20.sol#3) necessitates a version too
recent to be trusted. Consider deploying with 0.6.12/0.7.6
Pragma version^0.8.0 (node_modules/@openzeppelin/contracts/token/ERC20/extensions/ERC20Burnable.sol#3) necessita
tes a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6
Pragma version^0.8.0 (node_modules/@openzeppelin/contracts/token/ERC20/extensions/IERC20Metadata.sol#3) necessit
ates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6
Pragma version^0.8.0 (node_modules/@openzeppelin/contracts/utils/Context.sol#3) necessitates a version too recen
t to be trusted. Consider deploying with 0.6.12/0.7.6
Pragma version^0.8.0 (node_modules/@openzeppelin/contracts/utils/math/SafeMath.sol#3) necessitates a version too
 recent to be trusted. Consider deploying with 0.6.12/0.7.6
Pragma version^0.8.0 (contracts/token.sol#2) necessitates a version too recent to be trusted. Consider deploying
 with 0.6.12/0.7.6
solc-0.8.4 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Detectors:
Parameter OBToken.setFee(uint256).fee_divider (contracts/token.sol#38) is not in mixedCase
Variable OBToken._fee_divider (contracts/token.sol#21) is not in mixedCase
Variable OBToken._dev_wallet (contracts/token.sol#22) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventi
ons
```

```
INFO:Detectors:
OBToken._transfer(address,address,uint256) (contracts/token.sol#68-95) performs a multiplication on the result o
f a division:
        -amount -= (fee / 2) * 2 (contracts/token.sol#92)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#divide-before-multiply
INFO:Detectors:
OBToken.setDevWallet(address).addr (contracts/token.sol#33) lacks a zero-check on :
                - _dev_wallet = addr (contracts/token.sol#34)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-zero-address-validation
INFO:Detectors:
OBToken._transfer(address,address,uint256) (contracts/token.sol#68-95) uses timestamp for comparisons
        Dangerous comparisons:
        - vestindex < _vestingschedules[vestid].length (contracts/token.sol#81)
        - require(bool,string)(balance_left > _vestingschedules[vestid][vestindex],Amount to transfer is not all
owed by the vesting scheme) (contracts/token.sol#83)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#block-timestamp
```

Mythril

Mythril is a security analysis tool for EVM bytecode. It detects security vulnerabilities in smart contracts built for Ethereum, Hedera, Quorum, Vechain, Roostock, Tron, and other EVM-compatible blockchains. It uses symbolic execution, SMT solving, and taint analysis to detect a variety of security vulnerabilities.

```
==== Dependence on predictable environment variable ====
SWC ID: 116
Severity: Low
Contract: OBToken
Function name: transfer(address,uint256)
PC address: 5077
Estimated Gas Usage: 4844 - 5509
A control flow decision is made based on The block.timestamp environment variable.
The block.timestamp environment variable is used to determine a control flow decision. Note that the values of v
ariables like coinbase, gaslimit, block number and timestamp are predictable and can be manipulated by a malicio
us miner. Also keep in mind that attackers know hashes of earlier blocks. Don't use any of those environment var
iables as sources of randomness and be aware that use of these variables introduces a certain level of trust int
o miners.
--------------------
In file: #utility.yul:227

if lt(x, y) { panic_error_0x11() }

--------------------
```

```
SWC ID: 116
Severity: Low
Contract: OBToken
Function name: transfer(address,uint256)
PC address: 3034
Estimated Gas Usage: 5821 - 6676
A control flow decision is made based on The block.timestamp environment variable.
The block.timestamp environment variable is used to determine a control flow decision. Note that the values of v
ariables like coinbase, gaslimit, block number and timestamp are predictable and can be manipulated by a malicio
us miner. Also keep in mind that attackers know hashes of earlier blocks. Don't use any of those environment var
iables as sources of randomness and be aware that use of these variables introduces a certain level of trust int
o miners.
--------------------
In file: contracts/token.sol:81

if (vestindex < _vestingschedules[vestid].length) {
                uint256 balance_left = senderBalance - amount;
                require(balance_left > _vestingschedules[vestid][vestindex], "Amount to transfer is not allowed
by the vesting scheme");
            }
```

Limitations on Disclosure and Use of this Report

This report contains information concerning potential details of OBToken and methods for exploiting them. Antier Solutions recommends that precautions should be taken to protect the confidentiality of this document and the information contained herein.

Security Assessment is an uncertain process based on experiences, currently available information, and known threats. All information security systems, which by their nature are dependent on human beings, are vulnerable to some degree. Therefore, although Antier Solutions has identified major security vulnerabilities of the analyzed system, there can be no assurance that any exercise of this nature will identify all possible vulnerabilities or propose exhaustive and operationally viable recommendations to mitigate those exposures.

As technologies and risks change over time, the vulnerabilities associated with the operation of the OBToken Smart Contract described in this report, as well as the actions necessary to reduce the exposure to such vulnerabilities will also change. Antier Solutions makes no undertaking to supplement or update this report based on the changed circumstances or facts of which Antier Solutions becomes aware after the date hereof.

This report may recommend that Antier Solutions use certain software or hardware products manufactured or maintained by other vendors. Antier Solutions bases these recommendations on its prior experience with the capabilities of those products. Nonetheless, Antier Solutions does not and cannot warrant that a particular product will work as advertised by the vendor, nor that it will operate in the manner intended.

The Non-Disclosure Agreement (NDA) in effect between Antier Solutions and OB Trading B.V. governs the disclosure of this report to all other parties, including product vendors and suppliers.