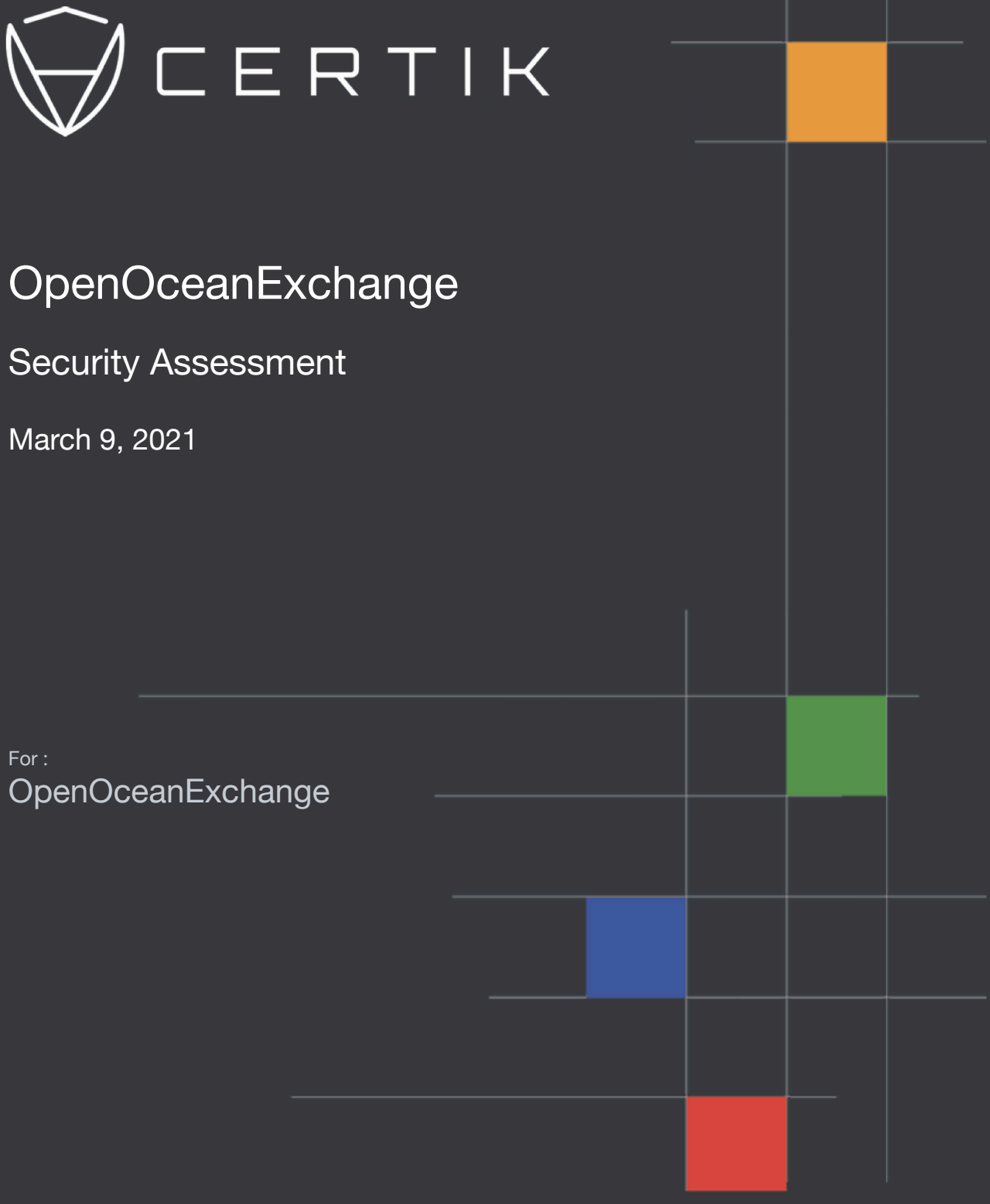


OpenOceanExchange

Security Assessment

March 9, 2021

For :
OpenOceanExchange

Disclaimer

CertiK 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 or project that contracts CertiK to perform a security review.

CertiK Reports 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 technologies proprietors, business, business model or legal compliance.

CertiK Reports 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.

CertiK 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. CertiK’s position is that each company and individual are responsible for their own due diligence and continuous security. CertiK’s goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

What is a CertiK report?

- A document describing in detail an in depth analysis of a particular piece(s) of source code provided to CertiK by a Client.
- An organized collection of testing results, analysis and inferences made about the structure, implementation and overall best practices of a particular piece of source code.
- Representation that a Client of CertiK has indeed completed a round of auditing with the intention to increase the quality of the company/product’s IT infrastructure and or source code.

Overview

Project Summary

Project Name	OpenOceanExchange
Description	Defi
Platform	Ethereum; Bsc; Tron; Solidity;
Codebase	GitHub Repository
Commits	9838ba65d67e1dc4b1f9a658b96cc3ec7f612a8a

Audit Summary

Delivery Date	Mar. 9, 2021
Method of Audit	Static Analysis, Manual Review
Consultants Engaged	2
Timeline	Mar.1 - Mar.6, Mar.9, 2021

Vulnerability Summary

Total Issues	4
🔴 **Total Critical**	0
🟡 **Total Major**	0
🔵 **Total Minor**	0
🟢 **Total Informational**	4

Executive Summary

This report has been prepared for **OpenOceanExchange** smart contract to discover issues and vulnerabilities in the source code of their Smart Contract as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Dynamic Analysis, Static Analysis, and Manual Review techniques.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

File in Scope

ID	Contract	SHA-256 Checksum
OOE	OpenOceanExchange.full.sol	48b6722271eb1752649f43b71eeec3a9a1aad24a594d5c208f69f134de96daef

Documentation

The sources of truth regarding the operation of the contracts in scope were lackluster and are something we advise to be enriched to aid in the legibility of the codebase as well as project. To help aid our understanding of each contract's functionality we referred to in-line comments and naming conventions.

These were considered the specification, and when discrepancies arose with the actual code behaviour, we consulted with the **OpenOceanExchange** team or reported an issue.

Review Notes

Certain optimization steps that we pinpointed in the source code mostly referred to coding standards and inefficiencies.

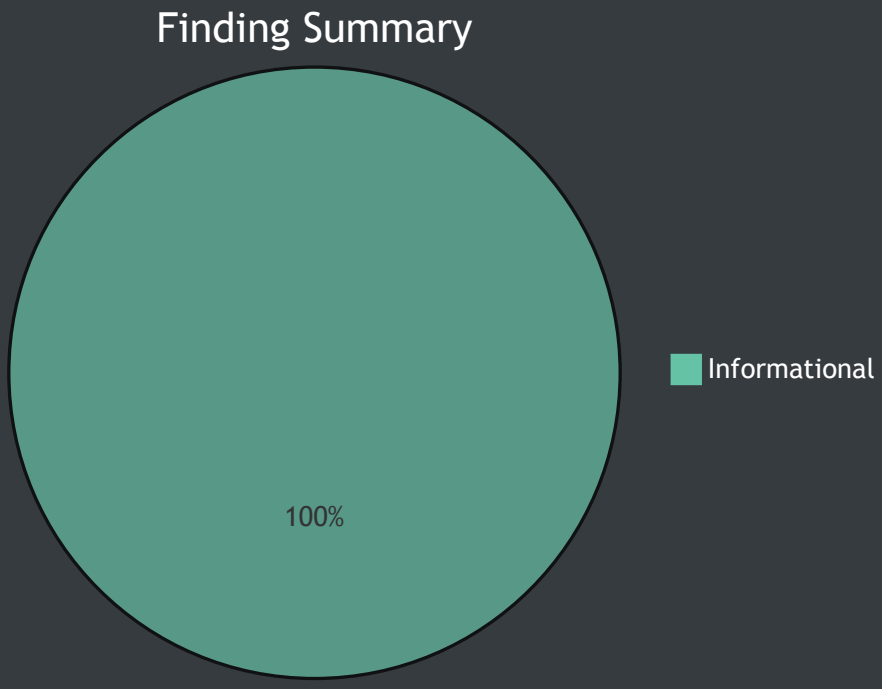
Certain discrepancies between the expected specification and the implementation of it were identified and were relayed to the team, however they pose no type of vulnerability and concern an optional code path that was unaccounted for.

The project has adequate documentation and specification outside of the source files, and the code comment coverage is good.

Recommendations

Overall, the codebase of the contracts should be refactored to assimilate the findings of this report, enforce linters and / or coding styles as well as correct any spelling errors and mistakes that appear throughout the code to achieve a high standard of code quality and security.

Findings



ID	Title	Type	Severity	Resolved
OOE-01	Unlocked Compiler Versions	Language Specific	Informational	!
OOE-02	Proper Usage of "public" and "external" Type	Gas Optimization	Informational	!
OOE-03	Local Variable Shadowing	Coding Style	Informational	!
OOE-04	Discussion For External Call	Optimization	Informational	✓

OOE-01: Unlocked Compiler Versions

Type	Severity	Location
Language Specific	Informational	OpenOceanExchange.full.sol L6,L248

Description:

An unlocked compiler version in the source code of the contract 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 an ambiguity when debugging as compiler specific bugs may occur in the codebase that would be hard to identify over a span of multiple compiler versions rather than a specific one.

Recommendation:

We advise that the compiler versions of entire codebase locked at the lowest version possible that the full project can be compiled at.

Alleviation:

No alleviation.

OOE-02: Proper Usage of "public" and "external" Type

Type	Severity	Location
Gas Optimization	Informational	OpenOceanExchange.full.sol L816

Description:

"public" functions that are never called by the contract could be declared "external" .

Examples:

Functions like : `OpenOceanExchange.swap()`

Recommendation:

Consider using the "external" attribute for functions never called from the contract. For example:

```
    function swap(
           ...
       ) external payable notShutdown returns (uint256 outAmount) {
           ...
       }
```

Alleviation:

No alleviation.

OOE-03: Local Variable Shadowing

Type	Severity	Location
Coding Style	Informational	OpenOceanExchange.full.sol L511,OpenOceanExchange.full.sol L796-L799

Description:

Constructor of contract `OpenOceanExchange` has a variable `_owner` :

```
        constructor(address _owner) public {
            spender = new TokenSpender();
            transferOwnership(_owner);
        }
```

Contract Ownable also has a variable `_owner` :

```
        address private _owner;
```

It's better to take different variable names to avoid confusion.

Recommendation:

Change the name of `_owner` in constructor of contract OpenOceanExchange.

Alleviation:

No alleviation.

OOE-04: Discussion For External Call

Type	Severity	Location
Optimization	Informational	OpenOceanExchange.full.sol L828-L834

Description:

There is an external call in Function `swap` .There is a potential security risk if malicious code is called.

```
        addressesToCall[i].externalCall(
                        gasLimitsAndValues[i] & ((1 << 128) - 1),
                        dataToCall,
                        offsets[i],
                        offsets[i + 1] - offsets[i],
                        gasLimitsAndValues[i] >> 128
                    )
```

Please check if this external call is safe.

Alleviation:

OpenOceanExchange Response : The external call function is provided by the OpenOceanExchange team, so it's safe.

Appendix

Finding Categories

Gas Optimization

Gas Optimization findings refer to exhibits that do not affect the functionality of the code but generate different, more optimal EVM opcodes resulting in a reduction on the total gas cost of a transaction.

Mathematical Operations

Mathematical Operation exhibits entail findings that relate to mishandling of math formulas, such as overflows, incorrect operations etc.

Logical Issue

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

Control Flow

Control Flow findings concern the access control imposed on functions, such as owner-only functions being invoke-able by anyone under certain circumstances.

Volatile Code

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

Data Flow

Data Flow findings describe faults in the way data is handled at rest and in memory, such as the result of a `struct` assignment operation affecting an in-memory `struct` rather than an instorage one.

Language Specific

Language Specific findings are issues that would only arise within Solidity, i.e. incorrect usage of `private` or `delete` .

Coding Style

Coding Style findings usually do not affect the generated byte-code and comment on how to make the codebase more legible and as a result easily maintainable.

Inconsistency

Inconsistency findings refer to functions that should seemingly behave similarly yet contain different code, such as a `constructor` assignment imposing different `require` statements on the input variables than a setter function.

Magic Numbers

Magic Number findings refer to numeric literals that are expressed in the codebase in their raw format and should otherwise be specified as `constant` contract variables aiding in their legibility and maintainability.

Compiler Error

Compiler Error findings refer to an error in the structure of the code that renders it impossible to compile using the specified version of the project.

Dead Code

Code that otherwise does not affect the functionality of the codebase and can be safely omitted.

Icons explanation

 : Issue resolved

 : Issue not resolved / Acknowledged. The team will be fixing the issues in the own timeframe.

 : Issue partially resolved. Not all instances of an issue was resolved.