Security Assessment

OgeeSwap AMM

Jul 7th, 2021

Table of Contents

Summary

Overview

- Project Summary
- Audit Summary
- Vulnerability Summary
- Audit Scope

Findings

- OFE-01 : Lack of Event Emissions for Significant Transactions
- ORE-01 : Incompatibility With Deflationary Tokens
- OTE-01 : Potential Integer Overflow

Appendix

Disclaimer

About

Summary

This report has been prepared for Ogee Finance to discover issues and vulnerabilities in the source code of the OgeeSwap AMM project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing 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.

The security assessment resulted in findings that ranged from critical to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices. We suggest recommendations that could better serve the project from the security perspective:

- Enhance general coding practices for better structures of source codes;
- Add enough unit tests to cover the possible use cases given they are currently missing in the repository;
- Provide more comments per each function for readability, especially contracts are verified in public;
- Provide more transparency on privileged activities once the protocol is live.

Overview

Project Summary

Project Name	OgeeSwap AMM
Platform	Heco
Language	Solidity
Codebase	
Commit	

Audit Summary

Delivery Date	Jul 07, 2021
Audit Methodology	Static Analysis, Manual Review
Key Components	

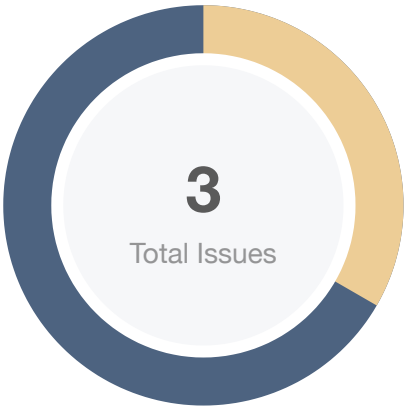
Vulnerability Summary

Vulnerability Level	Total	Pending	Partially Resolved	Resolved	Acknowledged	Declined
Critical	0	0	0	0	0	0
Major	0	0	0	0	0	0
Medium	0	0	0	0	0	0
Minor	1	1	0	0	0	0
Informational	2	2	0	0	0	0
Discussion	0	0	0	0	0	0

Audit Scope

ID	file	SHA256 Checksum
OFE	ogeeswap/OgeeswapFactory.sol	4b6579a5544567ccee8493440cc5f869daf6fba0172fc19f3a1d54089c2227f9
OGT	ogee-token	eb64e7f72fa59938dde4e172476563f29a6e5ec8940e3819f2008f04f258c980
OGE	ogeeswap	d6614737870dbf02db09737404b46d67e557ae2b6985f74478bc09737571ead2
OTE	ogee-token/OgeeToken.sol	9bbb8027727dd9a82295130f8db6616a0a53d69ae4c18625cc8ea139529637b1
ORE	ogeeswap/OgeeswapRouter.sol	390d65b4209c85fa0297431b340a02fb06ea9122b21484081af4e16e19bc3bf4

Findings



Critical	0 (0.00%)
Major	0 (0.00%)
Medium	0 (0.00%)
Minor	1 (33.33%)
Informational	2 (66.67%)
Discussion	0 (0.00%)

ID	Title	Category	Severity	Status
OFE-01	Lack of Event Emissions for Significant Transactions	Logical Issue	Informational	Pending
ORE-01	Incompatibility With Deflationary Tokens	Logical Issue	Minor	Pending
OTE-01	Potential Integer Overflow	Logical Issue	Informational	Pending

OFE-01 | Lack of Event Emissions for Significant Transactions

Category	Severity	Location	Status
Logical Issue	Informational	ogeeswap/OgeeswapFactory.sol: 530, 535	Pending

Description

The functions `OgeeswapFactory.setFeeTo()` and `OgeeswapFactory.setFeeToSetter()` involve significant transactions which would update the contract configurations. Missing event logs makes it difficult to track parameter or state changes.

Recommendation

We advise the client to emit events for the aforementioned functions.

ORE-01 | Incompatibility With Deflationary Tokens

Category	Severity	Location	Status
Logical Issue	Minor	ogeeswap/OgeeswapRouter.sol: 456, 455, 476, 495	Pending

Description

When users add or remove LP tokens into the router, and the `mint` and `burn` operations are performed. When transferring standard ERC20 deflationary tokens, the input amount may not be equal to the received amount due to the charged transaction fee. As a result, the amount inconsistency will occur and the transaction may fail due to the validation checks.

Recommendation

We advise the client to regulate the set of LP tokens supported and add necessary mitigation mechanisms to keep track of accurate balances if there is a need to support deflationary tokens.

OTE-01 | Potential Integer Overflow

Category	Severity	Location	Status
Logical Issue	Informational	ogee-token/OgeeToken.sol: 489	Pending

Description

`SafeMath.add()` is not used in the function `_writeCheckpoint()`, which might lead to integer overflow and cause potential incorrect processing result.

Recommendation

We advise the client to adopt `SafeMath.add()` to avoid potential integer overflow in the aforementioned function.

Appendix

Finding Categories

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.

Disclaimer

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to the Company in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes without CertiK's prior written consent.

This report is not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. This report is 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 assessment. This report does 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.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing 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.

About

Founded in 2017 by leading academics in the field of Computer Science from both Yale and Columbia University, CertiK is a leading blockchain security company that serves to verify the security and correctness of smart contracts and blockchain-based protocols. Through the utilization of our world-class technical expertise, alongside our proprietary, innovative tech, we're able to support the success of our clients with best-in-class security, all whilst realizing our overarching vision; provable trust for all throughout all facets of blockchain.