Security Assessment

OolongSwap

Oct 15th, 2021

Table of Contents

Summary

Overview

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

Findings

- OSF-01 : Lack of input validation
- OSF-02 : Centralization Risk
- OSP-01 : Mismatch of Codes and Comments
- OSP-02 : Centralization Risk
- OSR-01 : Proper Usage of `require` And `assert` Functions
- OSR-02 : Lack of input validation

Appendix

Disclaimer

About

Summary

This report has been prepared for OolongSwap to discover issues and vulnerabilities in the source code of the OolongSwap 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;
- Provide more comments per each function for readability, especially contracts that are verified in public;
- Provide more transparency on privileged activities once the protocol is live.

Overview

Project Summary

Project Name	OolongSwap
Platform	Ethereum
Language	Solidity
Codebase	https://github.com/OolongSwap/oolongswap-core/tree/903dd1166b6336b709c8873bb2c0ac43db5ca8a1/contracts
Commit	

Audit Summary

Delivery Date	Oct 15, 2021
Audit Methodology	Static Analysis, Manual Review
Key Components	

Vulnerability Summary

Vulnerability Level	Total	Pending	Declined	Acknowledged	Partially Resolved	Resolved
Critical	0	0	0	0	0	0
Major	2	0	0	2	0	0
Medium	0	0	0	0	0	0
Minor	0	0	0	0	0	0
Informational	4	0	0	4	0	0
Discussion	0	0	0	0	0	0

Audit Scope

ID	File	SHA256 Checksum
IER	interfaces/IERC20.sol	f665e903b98b0d76a0becad5fc84c03bd380b00edfa2bdc36ea424d46018e123
IOS	interfaces/IOolongSwapCallee.sol	58a2ad166f54b4dda1379a01a6d9540e713723b1cb2c87fa2a3d65b5a9b4e568
IOE	interfaces/IOolongSwapERC20.sol	50244578f26937d73a30313a323c97ef813fc32522b9dfc99f4c067ed3cabd3f
IOF	interfaces/IOolongSwapFactory.sol	c4823ca843c48a50fbde65cc9080b4786ee0773dff6e9fc0c5f286bb8d1c82ce
IOP	interfaces/IOolongSwapPair.sol	1bd1fcc2e0c5537d884427012f7532cd997a4578d037092c5d63da64d690acab
IOR	interfaces/IOolongSwapRouter01.sol	10acfe464c79561f500e9d42b53be18360ed34b2b658c376d8fb5cb0c9f2aa39
IOC	interfaces/IOolongSwapRouter02.sol	a56f1dd1dd0c9669b1a1292c4ebb031fe72fb7c7e42e59d1c7585899c479c047
IWE	interfaces/IWETH.sol	973ac9cc6853587679062600c304b5cb425fffd8ea1cfecc1b528f9782e9b265
MCK	libraries/Math.sol	e5e4a6f522b7ef72418e81874bb0e37646c7e6c9cd104c5e1d8cbaa13eb2fcc0
OSL	libraries/OolongSwapLibrary.sol	5e232f5eaa540299da7f1e80e0f34187f6a86cefca305277dd47b584c8ae8d06
SMC	libraries/SafeMath.sol	6d35be465dd8c9a5798d3eee87fd68e94fda06c378015d029d5d575248aa211b
THC	libraries/TransferHelper.sol	87ea8e943bc7a366b85869ae4e6973ef76238b943cced84219c47dd8fa1f5cb8
UQC	libraries/UQ112x112.sol	6c58c41fe1a59dd88cfc538d2366a26a312fea2dd21cc19f90ede6061dacbc5b
OSE	OolongSwapERC20.sol	19d196e906acf0562727ea307f619ec0fc5529f0375192a3af53015b13723d58

ID	File	SHA256 Checksum
OSF	OolongSwapFactory.sol	3fa955cb7a8312aefb18529d8a88d0c893f6d3d71a2482e6d71d6a8e8e2f85dd
OSP	OolongSwapPair.sol	d07e8cb5fcd606bc198853b7bfd3d6aa1e0a55f185a44a606fe764f2a7a16342
OSR	OolongSwapRouter02.sol	05b4729b213b7cc1239fee435a432b44e9493e393d44d97d1cb5f2f8bc754939

Findings

Critical	**0** (0.00%)
Major	**2** (33.33%)
Medium	**0** (0.00%)
Minor	**0** (0.00%)
Informational	**4** (66.67%)
Discussion	**0** (0.00%)

ID	Title	Category	Severity	Status
OSF-01	Lack of input validation	Volatile Code	Informational	Acknowledged
OSF-02	Centralization Risk	**Centralization / Privilege**	**Major**	Acknowledged
OSP-01	Mismatch of Codes and Comments	Coding Style	Informational	Acknowledged
OSP-02	Centralization Risk	**Centralization / Privilege**	**Major**	Acknowledged
OSR-01	Proper Usage of `require` And `assert` Functions	Language Specific	Informational	Acknowledged
OSR-02	Lack of input validation	Volatile Code	Informational	Acknowledged

OSF-01 | Lack of input validation

Category	Severity	Location	Status
Volatile Code	Informational	OolongSwapFactory.sol: 25	Acknowledged

Description

The assigned value to address type variable `_feeToSetter` should be verified as a non-zero value to prevent error.

Recommendation

Check that the address is not zero in the function as shown below:

```
require(_feeToSetter != address(0),"_feeToSetter is zero address!");
```

Alleviation

No Alleviation.

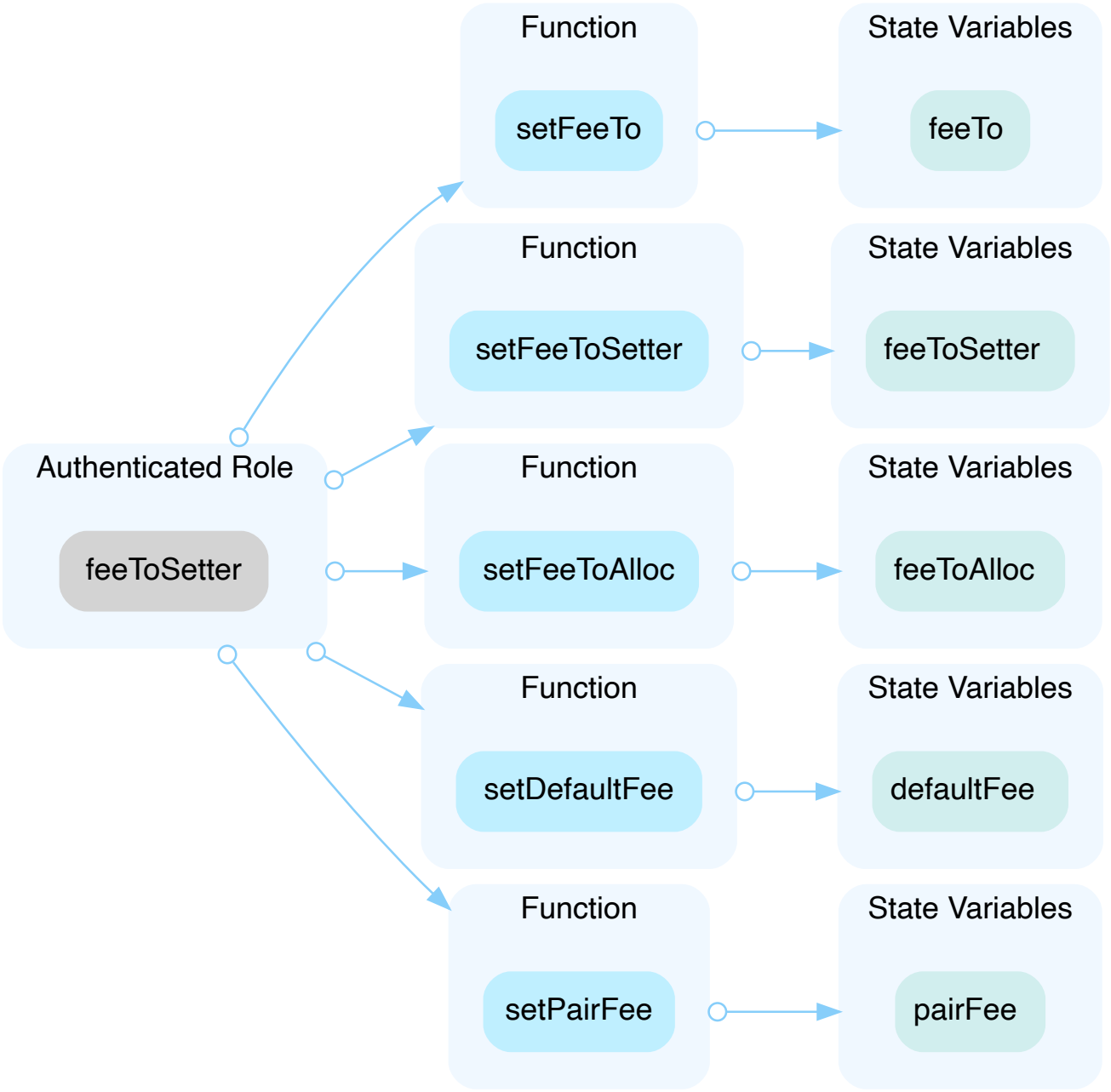
OSF-02 | Centralization Risk

Category	Severity	Location	Status
Centralization / Privilege	**Major**	OolongSwapFactory.sol: 57~60, 62~65, 67~71, 74~78, 81~85	Acknowledged

Description

In the contract, `OolongSwapFactory`, the role, `feeToSetter`, has the authority over the functions shown in the diagram below.

Any compromise to the privileged account which has access to `feeToSetter` may allow the hacker to take advantage of this.



Recommendation

We advise the client to carefully manage the privileged account's private key to avoid any potential risks of being hacked.

In general, we strongly recommend centralized privileges or roles in the protocol to be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., Multisignature wallets.

Indicatively, here is some feasible suggestions that would also mitigate the potential risk at the different level in term of short-term and long-term:

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to the private key;
- Introduction of a DAO/governance/voting module to increase transparency and user involvement.

Alleviation

The development team replied that they will solve it with multi sig wallet.

OSP-01 | Mismatch of Codes and Comments

Category	Severity	Location	Status
Coding Style	Informational	OolongSwapPair.sol: 89, 100	Acknowledged

Description

The comment says that the mint liquidity is equivalent to 1/6th of the growth in sqrt(k), but the statement implies not.

Alleviation

No Alleviation.

OSP-02 | Centralization Risk

Category	Severity	Location	Status
Centralization / Privilege	**Major**	OolongSwapPair.sol: 102	Acknowledged

Description

In the contract `OolongSwapPair`, the `feeTo` account would gain more and more fees when the `feeOn` is `true`. Any compromise to the `feeTo` account may allow the hacker to take advantage of this.

Recommendation

We advise the client to carefully manage the `feeTo` account's private key to avoid any potential risks of being hacked. In general, we strongly recommend centralized privileges or roles in the protocol to be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., Multisignature wallets.

Indicatively, here is some feasible suggestions that would also mitigate the potential risk at the different level in term of short-term and long-term:

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to the private key;
- Introduction of a DAO/governance/voting module to increase transparency and user involvement.

Alleviation

The development team replied that they will solve it with multi sig wallet.

OSR-01 | Proper Usage of `require` And `assert` Functions

Category	Severity	Location	Status
Language Specific	Informational	OolongSwapRouter02.sol: 30	Acknowledged

Description

The `assert` function should only be used to test for internal errors, and to check invariants. The `require` function should be used to ensure valid conditions, such as inputs, or contract state variables are met, or to validate return values from calls to external contracts.

Recommendation

We advise the client using the `require` function, along with a custom error message when the condition fails, instead of the `assert` function

Alleviation

No Alleviation.

OSR-02 | Lack of input validation

Category	Severity	Location	Status
Volatile Code	Informational	OolongSwapRouter02.sol: 25~26	Acknowledged

Description

The assigned values to address type variables `factory`, `WETH` should be verified as non-zero values to prevent error.

Recommendation

Check that the addresses are not zero in the constructor, like below:

```
require(_factory != address(0),"_factory is zero address!");
require(_WETH != address(0),"_WETH is zero address!");
```

Alleviation

No Alleviation.

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.

Volatile Code

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

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 but rather comment on how to make the codebase more legible and, as a result, easily maintainable.

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 you ("Customer" or 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, nor may copies be delivered to any other person other than the Company, without CertiK's prior written consent in each instance.

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.

The assessment services provided by CertiK is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.

ALL SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED "AS IS" AND "AS

AVAILABLE" AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, CERTIK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, CERTIK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, CERTIK MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER'S OR ANY OTHER PERSON'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE. WITHOUT LIMITATION TO THE FOREGOING, CERTIK PROVIDES NO WARRANTY OR UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KIND THAT THE SERVICE WILL MEET CUSTOMER'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE OR WORK WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS OR SERVICES, OPERATE WITHOUT INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

WITHOUT LIMITING THE FOREGOING, NEITHER CERTIK NOR ANY OF CERTIK'S AGENTS MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED AS TO THE ACCURACY, RELIABILITY, OR CURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE. CERTIK WILL ASSUME NO LIABILITY OR RESPONSIBILITY FOR (I) ANY ERRORS, MISTAKES, OR INACCURACIES OF CONTENT AND MATERIALS OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT, OR (II) ANY PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM CUSTOMER'S ACCESS TO OR USE OF THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS.

ALL THIRD-PARTY MATERIALS ARE PROVIDED "AS IS" AND ANY REPRESENTATION OR WARRANTY OF OR CONCERNING ANY THIRD-PARTY MATERIALS IS STRICTLY BETWEEN CUSTOMER AND THE THIRD-PARTY OWNER OR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS.

THE SERVICES, ASSESSMENT REPORT, AND ANY OTHER MATERIALS HEREUNDER ARE SOLELY PROVIDED TO CUSTOMER AND MAY NOT BE RELIED ON BY ANY OTHER PERSON OR FOR ANY PURPOSE NOT SPECIFICALLY IDENTIFIED IN THIS AGREEMENT, NOR MAY COPIES BE DELIVERED TO, ANY OTHER PERSON WITHOUT CERTIK'S PRIOR WRITTEN CONSENT IN EACH INSTANCE.

NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING

MATERIALS AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS.

THE REPRESENTATIONS AND WARRANTIES OF CERTIK CONTAINED IN THIS AGREEMENT ARE SOLELY FOR THE BENEFIT OF CUSTOMER. ACCORDINGLY, NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH REPRESENTATIONS AND WARRANTIES AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH REPRESENTATIONS OR WARRANTIES OR ANY MATTER SUBJECT TO OR RESULTING IN INDEMNIFICATION UNDER THIS AGREEMENT OR OTHERWISE.

FOR AVOIDANCE OF DOUBT, THE SERVICES, INCLUDING ANY ASSOCIATED ASSESSMENT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

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.