Tradoor Smart Contract Audit Report

Mon May 20 2024

contact@bitslab.xyz https://twitter.com/tonbit_

TonBit

Tradoor Smart Contract Audit Report

1 Executive Summary

1.1 Project Information

Description	Tradoor is a NDMM exchange
Type	DeFi
Auditors	TonBit
Timeline	Thu Apr 25 2024 - Mon May 20 2024
Languages	Tact
Platform	Ton
Methods	Architecture Review, Unit Testing, Manual Review
Source Code	https://github.com/TonTradoor/tradoor-contracts
Commits	3b7201c176270cfabb64944455ace94f55825e19 b950ec5c7edf9a484c2da47d001c262887e8f5c6 71b0b9fef91ae36bdc081fcb0bdc6ffd9f469196 af2f4caea9af889298edda8e62ab31bee467878c 27af022e3731ae58c9174c32987797baff4d4f4f f728fc713444697ee2cab96756cc45652eaad28a

1.2 Files in Scope

The following are the SHA1 hashes of the original reviewed files.

ID	File	SHA-1 Hash
STD	contracts/imports/stdlib.fc	2f104cd568a4cebb1c4112ecf8979800f0672575
STR	contracts/pool/structs.tact	e96260d35f8ee26117070b85fa5157eb1643f091
POO	contracts/pool/pool.tact	b0d82a5e2e4f880fb16e559baf9db93e38ea55e7
MES1	contracts/pool/messages.tact	8f9ca6e8ef96758554d35c56aef3494c2b3db15f
EVE	contracts/pool/events.tact	e5a56a79d3513949e9ed6b0270104bf15ea074c1
CON	contracts/pool/constants.tact	13486398e90e6a31938d9b35ee3e867fea591566
OBO	contracts/order/order_book.tact	8b54bd9148e691676a536762216f3b4030e38a2e
STR1	contracts/order/structs.tact	6136797c48cc561463d002b22c164899f1f505cc
MES2	contracts/order/messages.tact	362c1a3c7aee41d79ca74df69f47da8e1ef52c5a
EVE1	contracts/order/events.tact	e60be39667aca9ad1adf712e0c853d0f912563ff
CON1	contracts/order/constants.tact	265c53dc7e24f6637499def130d3c5a33fc46085

1.3 Issue Statistic

Item	Count	Fixed	Acknowledged
Total	13	13	0
Informational	1	1	0
Minor	4	4	0
Medium	3	3	0
Major	5	5	0
Critical	0	0	0

1.4 TonBit Audit Breakdown

TonBit aims to assess repositories for security-related issues, code quality, and compliance with specifications and best practices. Possible issues our team looked for included (but are not limited to):

- Transaction-ordering dependence
- Timestamp dependence
- Integer overflow/underflow by bit operations
- Number of rounding errors
- Denial of service / logical oversights
- Access control
- Centralization of power
- Business logic contradicting the specification
- Code clones, functionality duplication
- Gas usage
- Arbitrary token minting
- Unchecked CALL Return Values

1.5 Methodology

The security team adopted the **"Testing and Automated Analysis"**, **"Code Review"** strategy to perform a complete security test on the code in a way that is closest to the real attack. The main entrance and scope of security testing are stated in the conventions in the "Audit Objective", which can expand to contexts beyond the scope according to the actual testing needs. The main types of this security audit include:

(1) Testing and Automated Analysis

Items to check: state consistency / failure rollback / unit testing / value overflows / parameter verification / unhandled errors / boundary checking / coding specifications.

(2) Code Review

The code scope is illustrated in section 1.2.

(3) Audit Process

- Carry out relevant security tests on the testnet or the mainnet;
- If there are any questions during the audit process, communicate with the code owner in time. The code owners should actively cooperate (this might include providing the latest stable source code, relevant deployment scripts or methods, transaction signature scripts, exchange docking schemes, etc.);
- The necessary information during the audit process will be well documented for both the audit team and the code owner in a timely manner.

2 Summary

This report has been commissioned by TonTradoor to identify any potential issues and vulnerabilities in the source code of the Tradoor smart contract, as well as any contract dependencies that were not part of an officially recognized library. In this audit, we have utilized various techniques, including manual code review and static analysis, to identify potential vulnerabilities and security issues.

During the audit, we identified 13 issues of varying severity, listed below.

ID	Title	Severity	Status
OBO-1	Compensation Mechanisms May Introduce Centralization Risks	Medium	Fixed
POO-1	The `protocolTradingFee` Can't Be Withdrawn	Major	Fixed
POO-2	Never Updated Variable `unrealizedPnl` in `GlobalLPPosition`	Major	Fixed
POO-3	The Calculation Error when Updating Unrealized Profit and Loss	Major	Fixed
POO-4	The RrevPremiumRate Does Not Match With Token Type	Major	Fixed
POO-5	Update Global Liquidity Using Wrong Variable	Major	Fixed
POO-6	The Variable Clamped Funding Rate Delt Is Not Used	Medium	Fixed
POO-7	Bonus Calculation Formula Errors And Discrepancies	Medium	Fixed

POO-8	Meaningless If Statement	Minor	Fixed
POO-9	Redundant Code	Minor	Fixed
POO-10	Calculation Without Adding Funding Fee	Minor	Fixed
POO-11	Returns Incorrect Check Information	Minor	Fixed
POO-12	Variable That Can Not Be Updated	Informational	Fixed

Appendix 1

Issue Level

- **Informational** issues are often recommendations to improve the style of the code or to optimize code that does not affect the overall functionality.
- **Minor** issues are general suggestions relevant to best practices and readability. They don't post any direct risk. Developers are encouraged to fix them.
- **Medium** issues are non-exploitable problems and not security vulnerabilities. They should be fixed unless there is a specific reason not to.
- **Major** issues are security vulnerabilities. They put a portion of users' sensitive information at risk, and often are not directly exploitable. All major issues should be fixed.
- **Critical** issues are directly exploitable security vulnerabilities. They put users' sensitive information at risk. All critical issues should be fixed.

Issue Status

- **Fixed:** The issue has been resolved.
- **Partially Fixed:** The issue has been partially resolved.
- **Acknowledged:** The issue has been acknowledged by the code owner, and the code owner confirms it's as designed, and decides to keep it.

Appendix 2

Disclaimer

This report is based on the scope of materials and documents provided, with a limited review at the time provided. Results may not be complete and do not include 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 own risk. A report does not imply an endorsement of any particular project or team, nor does it guarantee its security. These reports should not be relied upon in any way by any third party, including for the purpose of making any decision to buy or sell products, services, or any other assets. TO THE FULLEST EXTENT PERMITTED BY LAW, WE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, IN CONNECTION WITH THIS REPORT, ITS CONTENT, RELATED SERVICES AND PRODUCTS, AND YOUR USE, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NOT INFRINGEMENT.