SECURITY AUDIT REPORT

for

Swarm Open dOTC

Prepared By: Xiaomi Huang

PeckShield

July 30, 2024

Document Properties

Client	Swarm
Title	Security Audit Report
Target	Swarm Open dOTC
Version	1.0
Author	Xuxian Jiang
Auditors	Daisy Cao, Xuxian Jiang
Reviewed by	Xiaomi Huang
Approved by	Xuxian Jiang
Classification	Public

Version Info

Version	Date	Author(s)	Description
1.0	July 30, 2024	Xuxian Jiang	Final Release
1.0-rc	July 27, 2024	Xuxian Jiang	Release Candidate #1

Contact

For more information about this document and its contents, please contact PeckShield Inc.

Name	Xiaomi Huang
Phone	+86 183 5897 7782
Email	contact@peckshield.com

Contents

1 Introduction

Given the opportunity to review the design document and related smart contract source code of the `Swam Open dOTC` protocol, we outline in the report our systematic approach to evaluate potential security issues in the smart contract implementation, expose possible semantic inconsistencies between smart contract code and design document, and provide additional suggestions or recommendations for improvement. Our results show that the given version of smart contracts can be further improved due to the presence of several issues related to either security or performance. This document outlines our audit results.

1.1 About Swarm Open dOTC

`Swarm Open dOTC` is proposed to provide a secure, decentralized platform for trading various types of digital assets without needing a centralized authority. This approach enhances transparency, security, and trust among participants while also leveraging blockchain technology to automate many aspects of traditional OTC trading. By using smart contracts, the platform can reduce the risk of fraud, speed up transactions, and decrease the costs associated with trading, thereby making it accessible to a broader range of participants globally. The basic information of audited contracts is as follows:

Table 1.1: Basic Information of Swarm Open dOTC

Item	Description
Name	Swarm
Type	Solidity
Language	EVM
Audit Method	Whitebox
Latest Audit Report	July 30, 2024

In the following, we show the Git repository of reviewed files and the commit hash value used in this audit.

- https://github.com/SwarmMarkets/open-dotc.git (c113613)

And here is the commit ID after all fixes for the issues found in the audit have been checked in:

- https://github.com/SwarmMarkets/open-dotc.git (7dda75e)

1.2 About PeckShield

PeckShield Inc. [7] is a leading blockchain security company with the goal of elevating the security, privacy, and usability of current blockchain ecosystems by offering top-notch, industry-leading services and products (including the service of smart contract auditing). We are reachable at Telegram (https://t.me/peckshield), Twitter (http://twitter.com/peckshield), or Email (contact@peckshield.com).

Table 1.2: Vulnerability Severity Classification

Impact			
High	Critical	High	Medium
Medium	High	Medium	Low
Low	Medium	Low	Low
	High	*Medium*	*Low*

Likelihood

1.3 Methodology

To standardize the evaluation, we define the following terminology based on OWASP Risk Rating Methodology [6]:

- Likelihood represents how likely a particular vulnerability is to be uncovered and exploited in the wild;
- Impact measures the technical loss and business damage of a successful attack;
- Severity demonstrates the overall criticality of the risk.

Likelihood and impact are categorized into three ratings: *H*, *M* and *L*, i.e., *high*, *medium* and *low* respectively. Severity is determined by likelihood and impact, and can be accordingly classified into four categories, i.e., *Critical*, *High*, *Medium*, *Low* shown in Table 1.2.

To evaluate the risk, we go through a list of check items and each would be labeled with a severity category. For one check item, if our tool or analysis does not identify any issue, the

Table 1.3: The Full List of Check Items

Category	Check Item
Basic Coding Bugs	Constructor Mismatch
	Ownership Takeover
	Redundant Fallback Function
	Overflows & Underflows
	Reentrancy
	Money-Giving Bug
	Blackhole
	Unauthorized Self-Destruct
	Revert DoS
	Unchecked External Call
	Gasless Send
	Send Instead Of Transfer
	Costly Loop
	(Unsafe) Use Of Untrusted Libraries
	(Unsafe) Use Of Predictable Variables
	Transaction Ordering Dependence
	Deprecated Uses
Semantic Consistency Checks	Semantic Consistency Checks
Advanced DeFi Scrutiny	Business Logics Review
	Functionality Checks
	Authentication Management
	Access Control & Authorization
	Oracle Security
	Digital Asset Escrow
	Kill-Switch Mechanism
	Operation Trails & Event Generation
	ERC20 Idiosyncrasies Handling
	Frontend-Contract Integration
	Deployment Consistency
	Holistic Risk Management
Additional Recommendations	Avoiding Use of Variadic Byte Array
	Using Fixed Compiler Version
	Making Visibility Level Explicit
	Making Type Inference Explicit
	Adhering To Function Declaration Strictly
	Following Other Best Practices

contract is considered safe regarding the check item. For any discovered issue, we might further deploy contracts on our private testnet and run tests to confirm the findings. If necessary, we would additionally build a PoC to demonstrate the possibility of exploitation. The concrete list of check items is shown in Table 1.3.

In particular, we perform the audit according to the following procedure:

- Basic Coding Bugs: We first statically analyze given smart contracts with our proprietary static code analyzer for known coding bugs, and then manually verify (reject or confirm) all the issues found by our tool.

- Semantic Consistency Checks: We then manually check the logic of implemented smart contracts and compare with the description in the white paper.

- Advanced DeFi Scrutiny: We further review business logics, examine system operations, and place DeFi-related aspects under scrutiny to uncover possible pitfalls and/or bugs.

- Additional Recommendations: We also provide additional suggestions regarding the coding and development of smart contracts from the perspective of proven programming practices.

To better describe each issue we identified, we categorize the findings with Common Weakness Enumeration (CWE-699) [5], which is a community-developed list of software weakness types to better delineate and organize weaknesses around concepts frequently encountered in software development. Though some categories used in CWE-699 may not be relevant in smart contracts, we use the CWE categories in Table 1.4 to classify our findings. Moreover, in case there is an issue that may affect an active protocol that has been deployed, the public version of this report may omit such issue, but will be amended with full details right after the affected protocol is upgraded with respective fixes.

1.4 Disclaimer

Note that this security audit is not designed to replace functional tests required before any software release, and does not give any warranties on finding all possible security issues of the given smart contract(s) or blockchain software, i.e., the evaluation result does not guarantee the nonexistence of any further findings of security issues. As one audit-based assessment cannot be considered comprehensive, we always recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contract(s). Last but not least, this security audit should not be used as investment advice.

Table 1.4: Common Weakness Enumeration (CWE) Classifications Used in This Audit

Category	Summary
Configuration	Weaknesses in this category are typically introduced during the configuration of the software.
Data Processing Issues	Weaknesses in this category are typically found in functionality that processes data.
Numeric Errors	Weaknesses in this category are related to improper calculation or conversion of numbers.
Security Features	Weaknesses in this category are concerned with topics like authentication, access control, confidentiality, cryptography, and privilege management. (Software security is not security software.)
Time and State	Weaknesses in this category are related to the improper management of time and state in an environment that supports simultaneous or near-simultaneous computation by multiple systems, processes, or threads.
Error Conditions, Return Values, Status Codes	Weaknesses in this category include weaknesses that occur if a function does not generate the correct return/status code, or if the application does not handle all possible return/status codes that could be generated by a function.
Resource Management	Weaknesses in this category are related to improper management of system resources.
Behavioral Issues	Weaknesses in this category are related to unexpected behaviors from code that an application uses.
Business Logics	Weaknesses in this category identify some of the underlying problems that commonly allow attackers to manipulate the business logic of an application. Errors in business logic can be devastating to an entire application.
Initialization and Cleanup	Weaknesses in this category occur in behaviors that are used for initialization and breakdown.
Arguments and Parameters	Weaknesses in this category are related to improper use of arguments or parameters within function calls.
Expression Issues	Weaknesses in this category are related to incorrectly written expressions within code.
Coding Practices	Weaknesses in this category are related to coding practices that are deemed unsafe and increase the chances that an exploitable vulnerability will be present in the application. They may not directly introduce a vulnerability, but indicate the product has not been carefully developed or maintained.

2 Findings

2.1 Summary

Here is a summary of our findings after analyzing the `Swarm Open dOTC` implementations. During the first phase of our audit, we study the smart contract source code and run our in-house static code analyzer through the codebase. The purpose here is to statically identify known coding bugs, and then manually verify (reject or confirm) issues reported by our tool. We further manually review business logics, examine system operations, and place DeFi-related aspects under scrutiny to uncover possible pitfalls and/or bugs.

Severity	# of Findings	
Critical	0	
High	0	
Medium	2	🟦 🟦
Low	3	🟦 🟦 🟦
Total	5	

We have so far identified a list of potential issues: some of them involve subtle corner cases that might not be previously thought of, while others refer to unusual interactions among multiple contracts. For each uncovered issue, we have therefore developed test cases for reasoning, reproduction, and/or verification. After further analysis and internal discussion, we determined a few issues of varying severities need to be brought up and paid more attention to, which are categorized in the above table. More information can be found in the next subsection, and the detailed discussions of each of them are in Section 3.

2.2 Key Findings

Overall, these smart contracts are well-designed and engineered, though the implementation can be improved by resolving the identified issues (shown in Table 2.1), including 2 medium-severity vulnerabilities and 3 low-severity vulnerabilities.

Table 2.1: Key Audit Findings

ID	Severity	Title	Category	Status
PVE-001	Low	Improved Gas Efficiency in Offer Cancellation inDotcEscrowV2	Coding Practices	Resolved
PVE-002	Low	Improved Validation on Fee Amount/Receiver Update	Coding Practices	Resolved
PVE-003	Medium	Strengthen offerPricingType/TakingOfferType Validation in DotcV2	Business Logic	Resolved
PVE-004	Medium	Trust Issue of Admin Keys	Security Features	Mitigated
PVE-005	Low	Suggested FeesReceiverSet Event Generation in DotcManagerV2	Coding Practices	Resolved

Beside the identified issues, we emphasize that for any user-facing applications and services, it is always important to develop necessary risk-control mechanisms and make contingency plans, which may need to be exercised before the mainnet deployment. The risk-control mechanisms should kick in at the very moment when the contracts are being deployed on mainnet. Please refer to Section 3 for details.

3 | Detailed Results

3.1 Improved Gas Efficiency in Offer Cancellation in DotcEscrowV2

- ID: PVE-001
- Severity: Low
- Likelihood: Low
- Impact: Low
- Target: DotcEscrowV2
- Category: Coding Practices [4]
- CWE subcategory: CWE-1126 [1]

Description

In the audited Swam Open dOTC protocol, there is a key DotcEscrowV2 contract that is designed to deposit, withdraw, and manage of assets in the course of trading. While examining the related trade offer cancellation logic, we notice the cancellation may be revised for improved gas efficiency.

In the following, we show the code snippet of the related cancelDeposit() routine. This routine has a rather straightforward logic in cancelling an offer. We notice the repeated uses of offer.depositAsset.amount (lines 173, 177, 182, and 184). And they may be revised to consistently use the local variable amountToCancel (lines 177).

```
170        function cancelDeposit(uint256 offerId, address maker) external onlyDotc returns (
               uint256 amountToCancel) {
171            EscrowDeposit memory offer = escrowDeposits[offerId];
172
173            if (offer.depositAsset.amount <= 0) {
174                revert AmountToCancelEqZero();
175            }
176
177            amountToCancel = offer.depositAsset.amount;
178
179            escrowDeposits[offerId].escrowOfferStatusType = EscrowOfferStatusType.
                   OfferCancelled;
180            escrowDeposits[offerId].depositAsset.amount = 0;
181
```

```
        _assetTransfer(offer.depositAsset, address(this), maker, offer.depositAsset.amount);

        emit OfferCancelled(offerId, maker, offer.depositAsset.amount);
    }
```

Listing 3.1: `DotcEscrowV2::cancelDeposit()`

Recommendation Revisit the above logic to use the local variable `amountToCancel` for gas efficiency.

Status The issue has been fixed by this commit: `b847927`.

3.2 Improved Validation on Fee Amount/Receiver Update

- ID: PVE-002
- Severity: Low
- Likelihood: Low
- Impact: Low

- Target: `DotcManagerV2`
- Category: Coding Practices [4]
- CWE subcategory: CWE-1126 [1]

Description

DeFi protocols typically have a number of system-wide parameters that can be dynamically configured on demand. The `Swam Open dOTC` protocol is no exception. Specifically, if we examine the `DotcManagerV2` contract, it has defined a number of protocol-wide risk parameters, such as `feeAmount` and `revSharePercentage`. In the following, we show the corresponding routines that allow for their changes.

```
    function changeFees(address _newFeeReceiver, uint256 _feeAmount, uint256 _revShare) external onlyOwner {
        if (_revShare > AssetHelper.SCALING_FACTOR) {
            revert IncorrectPercentage(_revShare);
        }

        feeReceiver = _newFeeReceiver;

        feeAmount = _feeAmount;

        revSharePercentage = _revShare;

        emit RevShareSet(msg.sender, _revShare);
        emit FeesAmountSet(msg.sender, _feeAmount);
        emit FeesReceiverSet(msg.sender, _newFeeReceiver);
    }
```

Listing 3.2: DotcManagerV2::changeFees()

These parameters define various aspects of the protocol operation and maintenance and need to exercise extra care when configuring or updating them. Our analysis shows the update logic on these parameters can be improved by applying more rigorous sanity checks. Based on the current implementation, certain corner cases may lead to an undesirable consequence. For example, the above routine can be improved to ensure feeReceiver will not be address(0) and _feeAmount will never be larger than 10 ** 27.

Recommendation Validate any changes regarding these system-wide parameters to ensure they fall in an appropriate range.

Status The issue has been fixed by this commit: 8d19141.

3.3 Strengthen offerPricingType/TakingOfferType Validation in DotcV2

- ID: PVE-003
- Severity: Medium
- Likelihood: Medium
- Impact: Medium
- Target: DotcV2
- Category: Coding Practices [4]
- CWE subcategory: CWE-1126 [1]

Description

To facilitate the trader offer management, Swam Open dOTC has defined a number of types and data structures. While examining two specific types, i.e., offerPricingType and TakingOfferType, we notice their enforcement in trade execution can be strengthened.

In the following, we shows the code snippet from the related takeOfferFixed() routine. This routine is used to take a fixed price offer. However, current logic does not validate the given offer (from the input offerId) is compliant with the indicated offer pricing type, i.e., OfferPricingType.FixedPricing. Moreover, current offer also has the so-called TakingOfferType that indicates whether the taker is allowed to take the full amount of assets or not. However, this TakingOfferType type is not enforced. The same issue is also applicable to the takeOfferDynamic() routine.

```
    function takeOfferFixed(uint256 offerId, uint256 withdrawalAmountPaid, address
        affiliate) external {
        DotcOffer memory offer = allOffers[offerId];
        offer.checkDotcOfferParams();
        offer.offer.checkOfferParams();

        if (withdrawalAmountPaid == 0  withdrawalAmountPaid > offer.withdrawalAsset.
            amount) {
            withdrawalAmountPaid = offer.withdrawalAsset.amount;
        }

        offer.withdrawalAsset.checkAssetOwner(msg.sender, withdrawalAmountPaid);

        uint256 withdrawalAssetAmount = withdrawalAmountPaid;
        ...
    }
```

Listing 3.3: `DotcV2::takeOfferFixed()`

Recommendation Improve the above-mentioned routines to honor the defined types, i.e., `offerPricingType` and `TakingOfferType`.

Status The issue has been fixed by this commit: `5191565`.

3.4 Trust Issue of Admin Keys

- ID: PVE-004
- Severity: Medium
- Likelihood: Low
- Impact: High

- Target: `DotcManagerV2`
- Category: Security Features [3]
- CWE subcategory: CWE-287 [2]

Description

In `Swam Open dOTC`, there is a privileged account `owner` (as well as the controlled operator). This account plays a critical role in governing and regulating the system-wide operations (e.g., configure parameters and update fees). Our analysis shows that this privileged account needs to be scrutinized. In the following, we use the `DotcManagerV2` contract as an example and show the representative functions potentially affected by the privileged account.

```
    function changeDotc(DotcV2 _dotc) external onlyOwner {
        if (address(_dotc) == address(0)) {
            revert ZeroAddressPassed();
        }

        dotc = _dotc;
        emit DotcAddressSet(msg.sender, _dotc);
    }
    ...
    function changeEscrow(DotcEscrowV2 _escrow) external onlyOwner {
        if (address(_escrow) == address(0)) {
            revert ZeroAddressPassed();
        }

        escrow = _escrow;
        emit EscrowAddressSet(msg.sender, _escrow);
    }
    ...
    function changeDotcInEscrow() external onlyOwner {
        escrow.changeDotc(dotc);
    }
    ...
    function changeEscrowInDotc() external onlyOwner {
        dotc.changeEscrow(escrow);
    }
    ...
    function changeFees(address _newFeeReceiver, uint256 _feeAmount, uint256 _revShare) external onlyOwner {
        if (_revShare > AssetHelper.SCALING_FACTOR) {
            revert IncorrectPercentage(_revShare);
        }

        feeReceiver = _newFeeReceiver;

        feeAmount = _feeAmount;

        revSharePercentage = _revShare;

        emit RevShareSet(msg.sender, _revShare);
        emit FeesAmountSet(msg.sender, _feeAmount);
        emit FeesReceiverSet(msg.sender, _newFeeReceiver);
    }
```

Listing 3.4: Privileged Operations in DotcManagerV2

We understand the need of the privileged functions for proper protocol operations, but at the same time the extra power to the owner may also be a counter-party risk to the protocol users. Therefore, we list this concern as an issue here from the audit perspective and highly recommend making these privileges explicit or raising necessary awareness among protocol users.

In the meantime, the protocol makes use of the proxy contract to allow for future upgrades. The upgrade is a privileged operation, which also falls in this trust issue on the admin key.

Recommendation Make the list of extra privileges granted to Dotc explicit to Whales Market users.

Status This issue has been mitigated as the team confirms the use of a multi-sig to manage the owner account.

3.5 Suggested FeesReceiverSet Event Generation in DotcManagerV2

- ID: PVE-005
- Severity: Low
- Likelihood: Low
- Impact: Low
- Target: DotcManagerV2
- Category: Coding Practices [4]
- CWE subcategory: CWE-1126 [1]

Description

In Ethereum, the event is an indispensable part of a contract and is mainly used to record a variety of runtime dynamics. In particular, when an event is emitted, it stores the arguments passed in transaction logs and these logs are made accessible to external analytics and reporting tools. Events can be emitted in a number of scenarios. One particular case is when system-wide parameters or settings are being changed. Another case is when tokens are being minted, transferred, or burned.

In the following, we examine the DotcManagerV2 contract and notice additional events may be emitted. Specifically, the following initialize() configures three important parameters, i.e., feeReceiver, feeAmount, and revSharePercentage. However, the related events, i.e., FeesReceiverSet, FeesAmountSet, and RevShareSet, are not emitted accordingly.

```
    function initialize(address _newFeeReceiver) public initializer {
        __Ownable_init(msg.sender);

        feeReceiver = _newFeeReceiver;
        feeAmount = 25 * (10 ** 23); // Default fee amount
        revSharePercentage = 8000; // Default revenue share percentage
    }
```

Listing 3.5: DotcManagerV2::initialize()

Recommendation Properly emit the following events when they are initialized: FeesReceiverSet , FeesAmountSet, and RevShareSet.

Status The issue has been fixed by this commit: 165f491.

4 Conclusion

In this audit, we have analyzed the `Swarm Open dOTC` design and implementation. It is proposed to provide a secure, decentralized platform for trading various types of digital assets without needing a centralized authority. This approach enhances transparency, security, and trust among participants while also leveraging blockchain technology to automate many aspects of traditional OTC trading. By using smart contracts, the platform can reduce the risk of fraud, speed up transactions, and decrease the costs associated with trading, thereby making it accessible to a broader range of participants globally. The current code base is well structured and neatly organized. Those identified issues are promptly confirmed and addressed.

Meanwhile, we need to emphasize that smart contracts as a whole are still in an early, but exciting stage of development. To improve this report, we greatly appreciate any constructive feedbacks or suggestions, on our methodology, audit findings, or potential gaps in scope/coverage.

References

[1] MITRE. CWE-1126: Declaration of Variable with Unnecessarily Wide Scope. https://cwe.mitre.org/data/definitions/1126.html.

[2] MITRE. CWE-287: Improper Authentication. https://cwe.mitre.org/data/definitions/287.html.

[3] MITRE. CWE CATEGORY: 7PK - Security Features. https://cwe.mitre.org/data/definitions/254.html.

[4] MITRE. CWE CATEGORY: Bad Coding Practices. https://cwe.mitre.org/data/definitions/1006.html.

[5] MITRE. CWE VIEW: Development Concepts. https://cwe.mitre.org/data/definitions/699.html.

[6] OWASP. Risk Rating Methodology. https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.

[7] PeckShield. PeckShield Inc. https://www.peckshield.com.