SECURITY AUDIT REPORT

for

Swarm Bundles

Prepared By: Xiaomi Huang

PeckShield

October 9, 2024

Document Properties

Client	Swarm
Title	Security Audit Report
Target	Swarm Bundles
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	October 9, 2024	Xuxian Jiang	Final Release

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 **4**

1.1 About Swarm Bundles 4

1.2 About PeckShield 5

1.3 Methodology 5

1.4 Disclaimer 7

2 Findings **9**

2.1 Summary 9

2.2 Key Findings 10

3 Detailed Results **11**

3.1 Improper Annual Fee Collection in xGoldBundle 11

3.2 Improved Mint/Burn Logic in BaseBundleToken 12

3.3 Trust Issue of Admin Keys 13

4 Conclusion **15**

References **16**

1 Introduction

Given the opportunity to review the design document and related smart contract source code of the `Swarm Bundles` 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 Bundles

`Swarm Bundles` is an ecosystem that enables unique assets to be composed into dynamic collections with similar assets which are then fractionalised for trading. Common use-cases include the bundling of non-fungible tokens representing real world assets such as stocks, carbon certificates, collectibles as well other unique physical and digital assets. Bundles diversify risk by allowing investors to buy into a collection of unique assets. A core property of Bundles is that they are not static collections, but can be augmented by adding and withdrawing assets through defined mechanisms. The basic information of audited contracts is as follows:

Table 1.1: Basic Information of Swarm Bundles

Item	Description
Name	Swarm
Type	Solidity
Language	EVM
Audit Method	Whitebox
Latest Audit Report	October 9, 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/swarm-nifty-bundles.git (db08d5b)

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

- https://github.com/SwarmMarkets/swarm-nifty-bundles.git (e8670ab)

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 \ Likelihood	*High*	*Medium*	*Low*
High	Critical	High	Medium
Medium	High	Medium	Low
Low	Medium	Low	Low

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.

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

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 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 Bundles` 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	1	
Total	3	

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 1 low-severity vulnerability.

Table 2.1: Key Audit Findings

ID	Severity	Title	Category	Status
PVE-001	Medium	Improper Annual Fee Collection in xGoldBundle	Business Logic	Resolved
PVE-002	Low	Improved Mint/Burn Logic in BaseBundleToken	Business Logic	Resolved
PVE-003	Medium	Trust Issue of Admin Keys	Security Features	Mitigated

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 Improper Annual Fee Collection in xGoldBundle

- ID: PVE-001
- Severity: Medium
- Likelihood: Medium
- Impact: Medium
- Target: `xGoldBundle`
- Category: Coding Practices [4]
- CWE subcategory: CWE-1126 [1]

Description

In the audited `Swarm Bundles` protocol, there is a key `xGoldBundle` contract that represents a bundle of `xGold`, where 1 token represents `1 ounce` (consisting of `xGoldOz` and `xGoldKg`). While examining the annual fee collection for the bundle management, we notice the logic may be improved.

In the following, we show the code snippet of the affected `addNewAssets()` routine. This routine has a rather straightforward logic in adding new asset to the bundle. However, the fee is collected after the asset bundle token is minted, which changes the total supply. We notice the annual fee collection depends on the total supply for the fee calculation. With that, there is a need to collect annual fee before the new bundle token is minted.

```
    function addNewAssets(Asset[] calldata _assets) external {
        uint256 toMint;
        for (uint256 i = 0; i < _assets.length; ) {
            _onlyWhitelistedAsset(_assets[i].assetAddress);

            toMint += bundleStorage.getGoldPrice(_assets[i].assetAddress);

            unchecked {
                ++i;
            }
        }

        mint_(msg.sender, toMint);
        _updateAnnualFeesRate();
        _depositAssets(_assets);
```

```
    }
```

Listing 3.1: `xGoldBundle::addNewAssets()`

Recommendation Revisit the above logic to update annual fee before new bundle token is minted. Note the same issue also affects another related routine `withdrawAssets()`.

Status The issue has been fixed by this commit: `f0559dd`.

3.2 Improved Mint/Burn Logic in BaseBundleToken

- ID: PVE-002
- Severity: Low
- Likelihood: Low
- Impact: Low
- Target: `BaseBundleToken`
- Category: Coding Practices [4]
- CWE subcategory: CWE-1126 [1]

Description

As mentioned earlier, the audited protocol charges certain fee for the bundle management. In the process of examining the fee deduction, we notice current logic to mint or redeem bundle token can be improved.

```
    function mint_(address to, uint256 amount) internal virtual {
        uint256 depositFees = AssetHelper.calculatePercentage(amount, bundleStorage.
            depositFeePercent());
        address feeReceiver = bundleStorage.feeReceiver();

        if (feeReceiver != address(0)) {
            _mint(feeReceiver, depositFees);
        }

        _mint(to, amount - depositFees);
    }
```

Listing 3.2: `BaseBundleToken::mint_()`

To elaborate, we show above the implementation of the `mint_()` routine. As the name indicates, this routine is used to mint new bundle tokens. Inside the mint logic, the deposit fee will be collected. It comes to our attention that if the deposit fee is non zero but the `feeReceiver` is not configured yet, the user is still deducted by the fee. With that, if the `feeReceiver` is not configured, the protocol is better off without deducting the deposit fee. Note the same improvement can also be applied to the `burn_()` routine.

Recommendation Revisit the above-mentioned routines to avoid fee deduction when the protocol has not configured the fee receiver yet.

Status The issue has been fixed by this commit: `257e919`.

3.3 Trust Issue of Admin Keys

- ID: PVE-003
- Severity: Medium
- Likelihood: Low
- Impact: High
- Target: `Multiple Contracts`
- Category: Security Features [3]
- CWE subcategory: CWE-287 [2]

Description

In `Swarm Bundles`, 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, whitelist assets, and collect annual fees). Our analysis shows that this privileged account needs to be scrutinized. In the following, we use the `xGold` contract as an example and show the representative functions potentially affected by the privileged account.

```
    function whitelistAssets(address[] calldata assets) external onlyOwner {
        require(assets.length <= IxGoldBundleStorage(bundleStorage).maxArraySize(),
            MaxArraySizeReached(assets.length));

        _whitelistAssets(assets);
    }

    /**
     * @notice Removes an asset from the whitelist.
     * @dev Only the contract owner can remove a whitelisted asset.
     * @param asset The address of the asset to remove from the whitelist.
     */
    function removeWhitelistedAsset(address asset) external onlyOwner {
        _removeWhitelistedAsset(asset);
    }

    /**
     * @notice Changes the BundleStorage contract associated with this bundle.
     * @dev Only the contract owner can change the bundle storage.
     * @param newBundleStorage The address of the new BundleStorage contract.
     */
    function changeBundleStorage(address newBundleStorage) external onlyOwner {
        _changeBundleStorage(newBundleStorage);
    }

    /**
```

```
     * @notice Updates the Know Your Asset (KYA) document for the bundle.
     * @dev Only the contract owner can update the KYA document.
     * @param kya The new KYA document or reference.
     */
    function updateKYA(string calldata kya) external onlyOwner {
        _updateKYA(kya);
    }
```

Listing 3.3: Privileged Operations in `xGold`

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.

Recommendation Make the list of extra privileges granted to `Dotc` explicit to protocol users.

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

4 Conclusion

In this audit, we have analyzed the design and implementation of `Swarm Bundles`, which is an ecosystem that enables unique assets to be composed into dynamic collections with similar assets which are then fractionalised for trading. Common use-cases include the bundling of non-fungible tokens representing real world assets such as stocks, carbon certificates, collectibles as well other unique physical and digital assets. Bundles diversify risk by allowing investors to buy into a collection of unique assets. A core property of Bundles is that they are not static collections, but can be augmented by adding and withdrawing assets through defined mechanisms. 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.