SB SECURITY

Kettle Mystery Box
Security Review

June 11, 2025

Contents

1. About SBSecurity

SBSecurity is a duo of skilled smart contract security researchers. Based on the audits conducted and numerous vulnerabilities reported, we strive to provide the absolute best security service and client satisfaction. While it's understood that 100% security and bug-free code cannot be guaranteed by anyone, we are committed to giving our utmost to provide the best possible outcome for you and your product.

Book a Security Review with us at sbsecurity.net or reach out on Twitter @Slavcheww.

2. Disclaimer

A smart contract security review can only show the presence of vulnerabilities **but not their absence**. Audits are a time, resource, and expertise-bound effort where skilled technicians evaluate the codebase and their dependencies using various techniques to find as many flaws as possible and suggest security-related improvements. We as a company stand behind our brand and the level of service that is provided but also recommend subsequent security reviews, on-chain monitoring, and high whitehat incentivization.

3. Risk classification

	Impact: High	Impact: Medium	Impact: Low
Likelihood: High	Critical	High	Medium
Likelihood: Medium	High	Medium	Low
Likelihood: Low	Medium	Low	Low

3.1. Impact

- **High** - leads to a significant loss of assets in the protocol or significantly harms a group of users.
- **Medium** - leads to a moderate loss of assets in the protocol or some disruption of the protocol's functionality.
- **Low** - funds are not at risk.

3.2. Likelihood

- **High** - almost **certain** to happen, easy to perform, or highly incentivized.
- **Medium** - only **conditionally possible**, but still relatively likely.
- **Low** - requires specific state or **little-to-no incentive**.

3.3. Action required for severity levels

- High - **Must** fix (before deployment if not already deployed).
- Medium - **Should** fix.
- Low - **Could** fix.

4. Executive Summary

Kettle Mystery Box contracts have been audited through the Hyacinth platform.

Overview

Project	Kettle Mystery Box
Repository	Private
Commit Hash	fdde845685849c9aa75cfd68951c96178466d634
Resolution	300e25379e5cfe593ff2a429c02c80039b6f0370
Timeline	June 10, 2025

Scope

MysteryBoxV2.sol
MysteryBoxRegistry.sol

Issues Found

Critical Risk	0
High Risk	0
Medium Risk	1
Low/Info Risk	0
Governance Risk	0

5. Findings

5.1. Medium severity

5.1.1. Mystery boxes can be griefed

Severity: Medium Risk

Description: Due to missing `onlyOwner` modifiers in the `registerMysteryBox` and `unregisterMysteryBox` functions of the `MysteryBoxRegistry`:

```
function registerMysteryBox(address mysteryBox) public {
    _isMysteryBox[mysteryBox] = true;
    emit BoxRegistered(mysteryBox, true);
}

function unregisterMysteryBox(address mysteryBox) public {
    _isMysteryBox[mysteryBox] = false;
    emit BoxRegistered(mysteryBox, false);
}
```

Anyone can use the functions to toggle the mystery boxes. If they're unregistered `onlyMysteryBox`, which is being used in the track functions, will be reverting, preventing the users from minting and revealing their prizes:

```
function mint(address minter) external {
    ...MORE CODE
    // Register the box with the registry
    registry.trackBox(tokenId, minter);
}
```

```
function trackBox(
    uint256 tokenId,
    address minter
) external onlyMysteryBox {//<---
    emit BoxTracked({
        boxContract: msg.sender,
        tokenId: tokenId,
        minter: minter
    });
}
```

Recommendation: Apply the `onlyOwner` modifier and set the new mystery boxes before their mint time opens.

Resolution: Fixed