SB SECURITY

Eden

Security Review

Nov 11, 2024

Conducted by:
Blckhv, Lead Security Researcher
Slavcheww, Lead Security Researcher

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

Eden is a DeFi token built on top of TitanX and Volt, utilizing a virtual mining model to power its ecosystem. The protocol offers staking options, allowing users to stake Eden for durations ranging from 90 to 1450 days, earning rewards in TitanX.

Overview

Project	Eden
Repository	Private
Commit Hash	3e92676df77da3a7e319f544554528d87e0a2d2a
Resolution	dea670ff8178cc6c66eb7a57ffa59c2b7ee567d3
Timeline	November 5 - November 10, 2024

Scope

src/*

Issues Found

Critical Risk	0
High Risk	0
Medium Risk	0
Low/Info Risk	5

5. Findings

5.1. Low/Info severity

5.1.1. amount for EdenBloom participation should be 195k Eden

Severity: Low Risk

Description: The amount for entering `EdenBloom` should be 195k Eden based on the docs and but it's still 150k like in Lotus.

Recommendation: Change the `EdenBloom` participation amount to 195k.

Resolution: Fixed

5.1.2. missing check for passing empty merkle root

Severity: Low Risk

Description: `LotusAirdrop` constructor is missing check if the Merkle tree root is not empty bytes.

Recommendation: Add check to revert if the `merkleRoot` is empty bytes.

Resolution: Fixed

5.1.3. EdenStaking uses block.ts as startTimestamp

Severity: Low Risk

Description: `EdenStaking` uses `block.timestamp` for start time, instead of setting exact block like `Minting` and `BuyAndBurn`.

Recommendation: Pass exact `block.timestamp` as `startTimestamp`.

Resolution: Fixed

5.1.4. Don't cast rewardPerShare calculation to uint160

Severity: Low Risk

Description: In `_updateRewards` do not cast to `uint160` the result that is added to `rewardPerShare` since the `rewardPerShare` is `uint256`.

Recommendation: Remove the casting to `uint160`.

Resolution: Fixed

5.1.5. `convertEdenToShares` assumes stakes for 1480 days are still possible

Severity: Low Risk

Description: Although now max staking duration is limited to 1450 days, convertEdenToShares is still passing 1480 as an `_upperBoundDays` and therefore will prevent stakes for the longest durations from receiving the maximal bonus.

Recommendation:

```
- else if (_duration <= 1480 days) {
+ else if (_duration <= 1450 days) {
            shares += uint160(
-               wmul(_amount, _Erank(_duration, 730 days, 1450 days, STAKING_ERANK_730DAYS,
STAKING_ERANK_1450DAYS))
+               wmul(_amount, _Erank(_duration, 730 days, 1450 days, STAKING_ERANK_730DAYS,
STAKING_ERANK_1450DAYS))
        );
```

Resolution: Fixed