vVv Vesting Staking Audit Report

Version 1.0

killua

vVv Vesting Staking Audit Report

killua

March 28, 2024

Prepared by: [killua]

Table of Contents

Table of Contents

Protocol Summary

vVv is the easiest way to gain exposure to the complete range of digital assets, including tokenized assets, real world assets, security tokens and cryptocurrencies. For more details

Disclaimer

The killua team makes all effort to find as many vulnerabilities in the code in the given time period, but holds no responsibilities for the findings provided in this document. A security audit by the team is not an endorsement of the underlying business or product. The audit was time-boxed and the review of the code was solely on the security aspects of the Solidity implementation of the contracts.

Risk Classification

		Impact		
		High	Medium	Low
Likelihood	High	H	H/M	M
	Medium	H/M	M	M/L
	Low	M	M/L	L

Scope

- Code Base: https://github.com/sherlock-audit/2024-03-vvv-vesting-staking

Issues found

Severity	Number of issues found
High	1
Medium	2
Low	0
Info	0
Gas Optimizations	0
Total	3

Findings

[H-01]Potential Loss of Unclaimed Vested Tokens upon Vesting Schedule Removal

Severity: High

Contract: VVVVesting

Function: removeVestingSchedule

Judging status: Invalidated

Description

The VVVVesting contract includes a function removeVestingSchedule that allows administrators to remove a user's vesting schedule. The vested tokens that have not yet been claimed by the user could become inaccessible if their vesting schedule is removed. This action could result in the loss of tokens that the user has rightfully earned according to the vesting terms.

Impact

If a vesting schedule is removed before a user has claimed their vested tokens, the user may be unable to claim their remaining tokens, effectively forfeiting them. This could lead to loss of trust in the platform.

Recommendation

- the Protocol should make arrangements for users to claim their vested tokens before removing a vesting schedule. This ensures that users receive the benefits they are entitled to and that the process is handled fairly and transparently.

[M-01]: Incorrect Configuration of Vesting Schedule parameters can lead to loss of functionality.

Severity : Medium impact: High likelihood: low (as admin is trusted) Judging status: Invalidated

Contract: VVVVesting.sol function: setVestingSchedule

Description: While centralization risk is acknowledged and Admin is trusted by the team, the _vestingScheduleCliffEndTime could be set to a value that is earlier than _vestingScheduleStartTime (by error/mistake),this could lead to - 1. immediate vesting of tokens that should be locked during the cliff period - 2. incorrect calculations of vested amounts. This inconsistency can cause an issue with the contract, not merely a Admin Privilege.

Impact
when cliffEndTime is set incorrectly,it causes: - premature release of tokens, affecting the token economy and potentially leading to loss of funds for the project.

Recommendation - We recommend implementing additional checks in setVestingSchedule function, to ensure that _vestingScheduleCliffEndTime is always greater than or equal to _vestingScheduleStartTime. for example: `require(_vestingScheduleCliffEndTime >= _vestingScheduleStartTime, "Cliff end time must be after schedule start time");`

[M-02]: Accumulated Precision Loss Due to Frequent Claiming of Staking Rewards

Severity: Medium

Contract: VVVETHStaking

Function: calculateAccruedVvvAmount, claimVvv Judging status: Invalidated

Description - The VVVETHStaking contract calculates the accrued VVV tokens for staked ETH using integer division, which results in truncation of any fractional token amounts. Our audit has identified that the frequency of claiming rewards can significantly impact the precision loss experienced by users. Specifically, users who claim their rewards more frequently, such as daily, will experience a higher cumulative loss over time due to the rounding down in each claim.

Impact

- While the loss in each individual claim may be a fraction of a VVV token, when claims are made frequently, these fractional losses can accumulate to a significant amount. For example, a user staking a large amount of ETH and claiming rewards daily could lose approximately 10 VVV tokens over a 90-day staking period due to rounding down.

Recommendation - We recommend reviewing the reward calculation and claim process to minimize precision loss. Potential solutions include:

- Fractional Tracking: Implement a system to track accrued fractions of tokens that are not claimed due to rounding and credit them in subsequent claims.