KyberPool
Security Analysis

by Pessimistic

This report is public.

Published: September 14, 2020

Abstract

In this report, we consider the security of the KyberPool project. Our task is to find and describe security issues in the smart contracts of the platform.

Disclaimer

The audit does not give any warranties on the security of the code. One audit cannot be considered enough. We always recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contracts. Besides, security audit is not an investment advice.

Summary

In this report, we considered the security of KyberPool smart contracts. We performed our audit according to the procedure described below.

The audit showed one medium-severity issue and several issues of low severity.

However, overall project quality is high.

General recommendations

We highly recommend fixing the medium-severity issue as it influences project's operation in current implementation. Also, we recommend fixing the low severity issues in order to increase the code quality and optimize gas consumption.

Procedure

In our audit, we consider the following crucial features of the code:

1. Whether the code is secure.
2. Whether the code corresponds to the documentation (including whitepaper).
3. Whether the code meets best practices.

We perform our audit according to the following procedure:

- manual audit
  - we manually analyze code base for security vulnerabilities
  - we assess overall project structure and quality
- report
  - we reflect all the gathered information in the report

Project overview

Project description

In our analysis we consider smart contracts of KyberPool project on Git repository, commit 4f15de9147521a23c92ae43ec2b000cc37a45973.

Project architecture

For the audit, we were provided with a git repository. The project has tests and documentation.

The total LOC of audited sources is 586.

Manual analysis

The contracts were completely manually analyzed, their logic was checked. Besides, the results of the automated analysis were manually verified. All the confirmed issues are described below.

Critical issues

Critical issues seriously endanger smart contracts security. We highly recommend fixing them.

The audit showed no critical issues.

Medium severity issues

Medium issues can influence project operation in current implementation. We highly recommend addressing them.

Missing check

`claimRewardsMaster` function does not check if the master has delegated his own stake. In this case, the reward of the pool should be split between its members excluding the master of the pool. However, the master is not excluded. Thus, `poolMembersShare` is less than it should be when the master's stake is delegated.

Low severity issues

Low severity issues can influence project operation in future versions of code. We recommend taking them into account.

Gas consumption

KyberPoolMaster.sol:

- lines 38-46: it is possible to combine two mappings into one `epoch -> feeHandler -> Struct`, where `Struct` contains `bool, uint, uint`. Moreover, one can use `uint248` to pack `bool + uint + uint` and thus, reduce the number of used storage slots.
- Line 333: if the `PoolMaster` changes fee frequently, then `delegationFees` array can grow significantly. Consider implementing binary search in `getEpochDFeeDataId()`.
- Line 466: `_epoch` to `delegationFees` computational complexity is currently $O(n^2)$. We recommend either
    - perform this calculation off-chain and only check the correctness on-chain or
    - require `_epochGroup` to be sorted, so that you can perform binary search to find the first occurrence of `DFeeData` and then move through the rest, in this case the complexity will be $O(n)$.

Code style

KyberPoolMaster.sol:

- Lines 354, 372: consider returning `DFeeData` struct instead (requires `ABIEncoderV2`).
- Line 393: `getUnclaimedRewards` should be view.
- Line 539: `applyFee(epochDFee);` should be called right after `epochDFee` declaration.
- Lines 521-536 and 765-775: `tokensWithRewards`/`findIndex` algorithm is suboptimal. Consider filling `accruedByToken` array for all `feeHandler`s instead and skip those with zero rewards when calling `sendTokens`.

`npm` commands in **README.md** file do not work in fresh environment (when `NODE_ENV` is not set).

Bad design

- The contract's most costly operations are `getAllEpochWithUnclaimedRewards() -> claimRewardsMaster()` and `_getAllEpochWithUnclaimedRewardsMember() -> _claimRewardsMember()` pairs of calls. These actions are difficult to design, which resulted in poor code quality.
  If the system does not have too many `feeHolder`s, redesigning these operations as `feeHolder`-dependant functions might improve the performance.
- Line 407: `rewardsPerEpoch` function is not present in `IKyberFeeHandler` interface, but only in the `KyberFeeHandler` contract, so you rely on implementation rather than abstraction.
- Line 606: there is an inconvenience in `getUnclaimedRewardsMember` logic. If `claimRewardsMaster` function has not been called for some epoch yet, the `getUnclaimedRewardsMember` function will ignore it. If a user calls the second variant of `getAllEpochWithUnclaimedRewardsMember` function (the one with `_fromEpoch`, `_toEpoch` arguments), rewards for some epochs might be missed.

This analysis was performed by Pessimistic:

Evgeny Marchenko, Senior Security Engineer
Boris Nikashin, Analyst
Alexander Seleznev, CEO

September 14, 2020