Smart Contract Audit

Vesper Strategies

Prepared for Bloq • April 2021

v210428

1. Executive Summary

In April 2021, Bloq engaged Coinspect to perform a source code review of a set of modifications performed to the Vesper platform. The objective of the audit was to continue evaluating the security of the smart contracts being developed.

The assessment was conducted on contracts from the Git repository at https://github.com/bloqpriv/vesper-pools obtained on **April 23**.

Overall, Coinspect did not find any high risk security vulnerabilities introduced by the modifications made to the Vesper since its previous audit that would result in stolen or lost user funds.

It is worth nothing that two new external dependencies were introduced by the changes in focus during this audit:

1. Keep3r network oracle
2. SushiSwap AMM

No issues were identified during the assessment:

High Risk	Medium Risk	Low Risk
0	0	0

The following report details the new changes introduced to the smart contracts and the tasks performed during this audit as well as suggestions aimed at improving the overall code quality and warnings regarding potential issues.

2. Introduction

The focus of this audit were several incremental changes performed to existing contracts and the recently added `VLINK` strategies and pool. The modifications introduced consisted in refactoring of strategies, new tests, and the addition of a new `SwapManager`.

The audit started on April 23rd and was conducted on the Git repository at https://github.com/bloqpriv/vesper-pools. The last commit reviewed during this engagement was `64005de6f98ae2d1d2f15fa02987d6358e570045` from **April 14th**:

```
commit 64005de6f98ae2d1d2f15fa02987d6358e570045
Merge: eecf92b 61d938d
Author: Kevin Beauregard <kbeau@regard.com>
Date:   Wed Apr 14 09:09:43 2021 -0700

   Merge pull request #501 from bloqpriv/swapmgrv1

   Swap Manager & VSP strategy update
```

The smart contracts that comprise the Vesper platform interact with multiple other contracts deployed by other projects which were not part of this review such as: MakerDAO, Uniswap, Compound and AAVE.

A new dependency on a price oracle from the Keep3r Network project (Keep3rV1Oracle | 0x73353801921417f465377c8d898c6f4c0270282c) was introduced by the latest changes and was not in scope for this audit. Also, the `SushiSwap` AMM will be utilized by the new `SwapManager` smart contract when choosing the best exchange rate for tokens in the Vesper platform.

A full review comprising these interactions should be performed in order to fully assess the security of the project.

3. Assessment

Vesper is a DeFi ecosystem and growth engine for crypto assets. It provides a suite of yield-generating products, focused on accessibility, optimization, and longevity.

The platform implements crypto asset pools that enable users to generate earnings using different strategies that supply liquidity to existing 3rd party pools in the DeFi ecosystem.

The code reviewed is currently under active development and consists of several pools and strategies which handle different types of collateral deposits and invest them in different projects.

This incremental audit performed as per Vesper request focused on a set of changes recently introduced to some of the contracts already audited in previous engagements, in order to establish if these modifications affected in any way the platform security.

As already mentioned in Coinspect's previous reports, most contracts are compiled with Solidity compiler version 0.6.12 and it is advised to migrate to a newer version whenever possible as this will increase protection from unknown vulnerabilities. Also using a newer compiler would result in gas usage optimizations, for example by using checked arithmetic and not requiring SafeMath. **The Coinspect team is aware that a new version of Vesper is being developed with an up-to-date compiler version.**

The following sections detail each of the code changes introduced by the commits reviewed by Coinspect.

3.1 New SwapManager and VSPStrategy update

The new `SwapManager.sol` smart contract was added. The `VSPStrategy.sol` contract was modified to instantiate an immutable `SwapManager` in its constructor, which is then used in the `_rebalanceEarned` function: instead of swapping via Uniswap, the best available exchange (from a list of exchanges included in the `SwapManager` contract) is utilized.

The `SwapManager` contract is similar to the `UniswapManager` recently introduced and reviewed in the previous audit, but allows comparing the expected trade result between a set of configured exchanges. The currently configured AMMs are `Uniswap` and `Sushiswap`.

Also, new tests related to the new functionality in `SwapManager` were added, including some tests that check for "sandwich attacks" when swapping tokens in the AMMs.

The following addresses referencing external contracts are used:

1. `0x7a250d5630B4cF539739dF2C5dAcb4c659F2488D` (`UniswapV2Router02` as listed in https://uniswap.org/docs/v2/smart-contracts/router02/)
2. `0xd9e1cE17f2641f24aE83637ab66a2cca9C378B9F` (`SushiV2Router02` as listed in https://dev.sushi.com/sushiswap/contracts)
3. `0x5C69bEe701ef814a2B6a3EDD4B1652CB9cc5aA6f` (`UniswapV2Factory` as listed in https://uniswap.org/docs/v2/smart-contracts/factory/)
4. `0xC0AEe478e3658e2610c5F7A4A2E1777cE9e4f2Ac` (`SushiV2Factory` as listed in https://dev.sushi.com/sushiswap/contracts)

The following commits implement this feature and were reviewed:

```
64005de Merge pull request #501 from bloqpriv/swapmgrv1
61d938d Swap Manager & VSP strategy update
```

3.2 Keep3r Oracle added to UniswapManager

Two public view functions were added to the previously reviewed `UniswapManager` contract. These functions call an external contract called `Keep3rV1Oracle`

(Keep3rV1Oracle | 0x73353801921417f465377c8d898c6f4c0270282c) which implements the `IUniswapV2Oracle` interface which was also added to the project repository. This address is listed in the Keep3r Network registry located in https://github.com/keep3r-network/keep3r.network/blob/master/REGISTRY.md.

The new functions added to `UniswapManager.sol` are called `getMinimumAcceptableOutput` and `oracleCurrent`. Both functions utilize the `Kee3rV1Oracle` contract `current` function, which according to a comment in the interface, returns the `amount out` corresponding to the `amount in` for a given token using the moving average over the time.

The new functions `are` not used by Vesper contracts yet.

The following commits implement this feature and were reviewed:

`eecf92b Merge pull request #497 from bloqpriv/keep3r-oracle`

`1fd07c2 Add Keep3r Oracle for Uni`

3.3 Mandatory _rebalanceDaiInLender implementation for MakerStrategy derived contracts

Replaced the `_withdrawExcessDaiFromLender` function call with a `_rebalanceDaiInLender` call in `_rebalanceEarned` in `MakerStrategy.sol`.

`CompounMakerStrategy.sol` and `VesperMakeStrategy.sol` were modified to reflect this change.

The following commit implements this change and was reviewed:

`bfcace6 make _rebalanceDaiInLender a required method for child contracts`

3.4 Added UniswapManager to MakerStrategy and CompoundMakerStrategy

The calls to the `_getAmountOut` function, which was removed, were replaced to now use the `UniswapManager bestPathFixedInput` function instead. In a similar fashion, the `uniswapRouter.swapExactTokensForTokens_` function calls were replaced with `_safeSwap` function calls. This function (which relies on the recently introduced `UniswapManager` contract) was added to `Strategy.sol` and is used now instead.

The internal `_rebalanceEarned` function was removed from `CompoundMakerStrategy.sol`.

Also, small refactoring changes were made to `MakerStrategy`, where a new internal `_paybackShortAmount` function called from _resurface was created. The function `_getPath` was not being used and was removed as well.

The following commits implement this feature and were reviewed:

`c955e16` `Merge pull request #493 from bloqpriv/uniswapify-maker`

`cbbb4bf` `Integrate UniMgr into MakerStrategy & CompoundMaker`

3.5 CompoundMakerStrategy fix

The `_claimReward` function visibility modifier was changed from public to internal.

The following commits implement this fix and were reviewed:

`bc508ad` `Merge pull request #489 from bloqpriv/minor-fix`

`bc49cf6` `Updated function modifier`

3.6 Tests refactoring and build environment changes

Only minor changes to the smart contracts were performed by these commits: error strings were replaced with shorter ones and unused code was removed. In addition, tests and the build environment were improved.

The following commits implement these changes and were reviewed:

`1370350` `Merge pull request #484 from bloqpriv/ghaction`

`6ba2142` `Using node url from env in GH action`

```
926f05c Merge pull request #483 from bloqpriv/test-update
a21bb87 Test fix, format fix
bd16f68 Updated tests
560284d Merge pull request #482 from bloqpriv/repo-cleanup
b5e3acf Removed warning and unused code
```

3.7 New vLink pool and related strategies

The new `VLINK.sol` pool and the new related strategies `AaveV2StrategyLINK.sol` and `VesperMakerStrategyLINK.sol` were added to the repository.
These contracts inherit from `VTokenBase`, `AaveV2Strategy` and `VesperMakerStrategy` respectively and do not implement any functionality themselves.

Coinspect verified the address `0x514910771af9ca656af840dff83e8264ecf986ca` used by the new contracts is the address of the Chainlink Token (LINK) as expected.

The following commits implement these modifications and were reviewed:

```
7afad3c Merge pull request #480 from bloqpriv/vLINK
b5f8237 vLink pool with vDai Compound
```

4. Disclaimer

The information presented in this document is provided "as is" and without warranty. Source code reviews are a “point in time” analysis and as such it is possible that something in the code could have changed since the tasks reflected in this report were executed. This report should not be considered a perfect representation of the risks threatening the analyzed system.